PASSMARK® SOFTWARE

Schnelle und effektive Endpoint-Security für Unternehmen

Eine vergleichende Analyse

Dokument: Schnelle und effektive Endpoint-Security für Unternehmen - Eine vergleichende Analyse
Autoren: K. Lai, D. Wren
Ausgabe: 1. Ausgabe
Datei: Fast and Effective Security for Business – Ed1 June 2010.pdf

Inhaltsverzeichnis

Inhaltsverzeichnis 2

Überarbeitungen. 3

Referenzen. 3

Einleitung. 4

Bewertungen und Resümee 5

Bewertungskategorien 6

Beschreibung der Bewertung mittels Sterne 6

Vorgehensweise von Passmark Software 7

Ergebnisse Benchmark Leistungstest. 8

ESET SMART SECURITY BUSINESS EDITION 11

KASPERSKY BUSINESS SPACE SECURITY 14

MCAFEE TOTAL PROTECTION FOR ENDPOINT 17

MICROSOFT FOREFRONT CLIENT SECURITY 20

SOPHOS ENDPOINT SECURITY AND DATA PROTECTION 23

SYMANTEC ENDPOINT PROTECTION 26

TREND MICRO WORRY FREE BUSINESS SECURITY 29

Haftungsausschluss und Bekanntmachung. 32

Haftungsausschluss 32

Bekanntmachung 32

Warenzeichen 32

Kontakt 32

Anhang A – Methodologie der Leistungsmessung 33

Überarbeitungen

Ausgabe	Historie	Datum
Edition 1	Erste Ausgabe des Dokuments. Charts der Leistungsmessung und vergleichende Artikel wurden hinzugefügt.	15. Juni 2010

Referenzen

Referenz	Dokument	Autor	Datum
1	AV Comparatives - Summary Report 2009 Aktuelle Version: Dezember 2009 Die Informationen aus diesem aktuellen Report wurden genutzt, um die Effektivität der getesteten Produkte bewerten zu können.	AV Comparatives	24. Dezember 2009
2	AV Comparatives - On-Demand Comparatives Aktuelle Version: Report Nummer 25, Februar 2010 Die Informationen aus diesem aktuellen Report wurden genutzt, um die Effektivität der getesteten Produkte bewerten zu können.	AV Comparatives	17. März 2010
3	AV Comparatives – Retrospective/ProActive Test Aktuelle Version: Report Number 26, Mai 2010 Die Informationen aus diesem aktuellen Report wurden genutzt, um die Effektivität der getesteten Produkte bewerten zu können.	AV Comparatives	5. Juni 2010
4	VB100 Test Results Current results: Windows Server 2008 R2, Juni 2010 Die Testergebnisse der Virus Bulletin wurden genutzt, um die Effektivität der getesteten Produkte bewerten zu können.	Virus Bulletin	Juni 2010
5	Network Traffic Monitor v2.01 Dieses Tool misst das ein- und ausgehende Datenvolumen. Dadurch konnte die Update-Größe bestimmt werden.	Nico Cuppen Software	-

Einleitung

Betrachtet man den Schaden, den Malware jährlich anrichtet und die Kosten, die Unternehmen für dessen Behebung aufbringen müssen, darf der Stellenwert einer effektiven Sicherheitslösung im Business-Umfeld nicht unterschätzt werden[1]. Immer ausgefeiltere Schädlinge bedrohen die Produktivität und den Ruf angegriffener Unternehmen.
Zudem bergen die immer mehr werdenden Angriffe die Gefahr großer Verluste durch Datendiebstahl und das Ausnutzen von Sicherheitslücken[2].

Als Antwort darauf vertrauen Unternehmen einer Reihe von unterschiedlichen Sicherheitslösungen, die den individuellen Security-Anforderungen gerecht werden. Aufgrund der großen Anzahl von verfügbarer Software vieler Hersteller stehen Unternehmen vor der Herausforderung, diejenige Sicherheitslösung zu finden, die am effektivsten vor Malware schützt, die Kosten für die Implementierung minimiert und geringen Einfluss auf betriebliche Funktionen und den Workflow ausübt.

Dieser Report fasst die Test-Ergebnisse von sieben Sicherheitslösungen der sieben weltweit größten Hersteller bezüglich Leistungsfähigkeit, Effektivität und Bedienung zusammen. In diesem Bericht hat PassMark Software die folgenden Business Security-Produkte untersucht:

- ESET Smart Security 4 Business Edition
- Kaspersky Business Space Security
- McAfee Total Protection for Endpoint
- Microsoft Forefront Client Security
- Symantec Endpoint Protection
- Sophos Endpoint Security and Data Protection
- Trend Micro Worry-Free Business Security: Standard Edition

[1] Eine in 2007 durchgeführte Umfrage der „Computer Economics Inc“ ergab, dass Malware Unternehmens-Schäden in Höhe von schätzungsweise 13 Mrd. Dollar pro Jahr verursachen.

[2] Der fünfte jährliche Report „Cost of a Data Breach“ des Ponemon Institue (Januar 2010) beziffert die durchschnittlichen Kosten für Datenmissbrauch bei 204 US-Dollar pro betroffenen Datensatz.

Bewertungen und Resümee

Passmark Software hat jedes Sicherheitsprodukt hinsichtlich der Gesamtleistung, der Benutzerfreundlichkeit, des Designs, der Funktionen und des Leistungsniveaus in den entsprechenden Kategorien bewertet. Diese stehen für die Hauptfunktionen oder wichtigsten Merkmale, die für Sicherheitssoftware in Business-Netzwerken üblich sind. Die Bewertungen reflektieren die subjektive Sicht und die Erfahrungen von Passmark Software hinsichtlich Installation, Konfiguration und Benutzung der Sicherheitsprodukte für Endpoints.

Die folgende Tabelle fasst die Bewertungen in allen Kategorien für jedes getestete Produkt zusammen.

	ESET	Kaspersky	McAfee	Microsoft	Sophos	Symantec	Trend Micro
Gesamtwertung	4.5	4	4.5	2	4.5	4	4.5
Installation & Konfiguration	4	4.5	3	1	4.5	4.5	4.5
Migration	4.5	5	2	1	5	4.5	5
Standard-Policies	4.5	4	4.5	2	4.5	4.5	4
Installation auf Clients	4	5	3	1	3	3	4.5
Design der Programmoberfläche	4	5	4.5	2.5	1.5	4.5	2.5
Management von Clients und Policies	5	4	5	1.5	3	4	3
RemoteManagement	4.5	5	4.5	--	4	4.5	4
Updates	4	2.5	4	2	1.5	5	4.5
Typische Anwendungsfälle	5	5	3	2	4.5	4.5	3
Effektivität	5	4.5	4.5	4	4.5	5	2
Leistungsfähigkeit	4.5	4	2.5	2	3	4	2

Bewertungskategorien

Die folgende Tabelle erklärt die Kriterien und Faktoren, die zur Bewertung jeder Business Sicherheitslösung pro Kategorie herangezogen wurden. Die Kategorien wurden vor den Tests festgelegt und entsprechend den Erwartungen an typische Features und Funktionen von Business Sicherheitssoftware ausgewählt.

Kategorie	Kategorie-Beschreibung
Gesamtbewertung	Die Bewertung für diese Kategorie errechnet sich zu gleichen Teilen aus dem Durchschnitt aller anderen Bewertungen.
Installation & Konfiguration	In dieser Kategorie werden Geschwindigkeit und Einfachheit der Installation und Konfiguration von Serverkomponenten bewertet. Dazu gehören die Qualität und Exaktheit der Dokumentation, die Möglichkeit zur Installation von Voreinstellungen, sowie die Güte der Integration des Installationsprogramms.
Migration	Diese Kategorie bewertet die Möglichkeit und Einfachheit der Produktmigration ausgehend von vorherigen Versionen oder der Software eines Fremdanbieters. Zusätzlich werden Anbieter hervorgehoben, die den Migrationsprozess verständlich dokumentiert haben.
Standard-Policies	Diese Kategorie bewertet aus der Sicht des Administrators den Nutzen von Grundeinstellungen, die während der Installation eingerichtet werden. Dabei wird auch überprüft, ob verschiedene Grundeinstellungen wählbar sind.
Client Installation	Diese Kategorie bewertet den Schwierigkeitsgrad der Installation auf dem Client hinsichtlich der Schnelligkeit der Verteilung und den Auswirkungen der Installation auf Endpoint-Nutzer.
Design der Programmoberfläche	Diese Kategorie bewertet die Funktionalität, intuitive Bedienung, Stabilität und Reaktionsgeschwindigkeit der Benutzeroberfläche.
Management von Clients und Policies	Diese Kategorie prüft die Flexibilität und Beschaffenheit der Regelverwaltung von der Serverkonsole aus. Dabei werden als Kriterien die Automatisierung der Gruppenerstellung und der Tiefe der Einstellungsmöglichkeiten für Administratoren herangezogen.
Remote Management	In dieser Kategorie wird bewertet, in welchem Ausmaß Administratoren dabei unterstützt werden, die Management-Konsole von einem anderen Arbeitsplatz aus bedienen zu können.
Updates	Diese Kategorie bewertet den Konfigurationsaufwand, damit Management-Server die zentrale Datenbank aktualisieren können, sowie die einfache Verteilung auf und die Abrufzeiten von Endpoint-Geräten.
Typische Anwendungsfälle	Diese Kategorie untersucht die Benutzerfreundlichkeit jedes Sicherheitsprodukts in drei typischen Anwendungsfällen. Die Szenarien sind: eine On-Demand Prüfung ausgewählter Endpoints, die Erstellung und Ansicht eines On-Demand Malwareberichts, sowie die Erstellung, Zuweisung und Verteilung einer neuen Policy.
Effektivität	Diese Kategorie bewertet die Anti-Malware Effektivität des Sicherheitsprodukts basierend auf aktuell veröffentlichten Informationen auf namhaften Testseiten. Es wird sich auf die Quellen VB 100 und AV Comparatives bezogen.
Performance	Diese Kategorie ist eine Gesamtbewertung der Leistung basierend auf zehn Benchmark Leistungstests, die von Passmark Software durchgeführt wurden.

Beschreibung der Bewertung mittels Sterne

Die folgende Tabelle beschreibt die allgemeine Bedeutung der Wertung hinsichtlich der Produktperformance, Bedienfreundlichkeit und Funktionalität.

Sternbewertung	Beschreibung der Wertung
--	**Nicht unterstützt** – In der Business Sicherheitslösung wird diese Kategorie nicht unterstützt. Weder im Handbuch noch in den Hilfedateien oder einer Onlinehilfe wird die Kategorie gefunden.
★	**sehr schwach** – Die Sicherheitslösung zeigte eine sehr eingeschränkte Leistung in dieser Kategorie. Produkte mit dieser Bewertung zeigten fehlende oder ungenaue Dokumentationen, sehr schlechte Bedienbarkeit oder technische Probleme, die die Produktstabilität, - Handhabung oder Funktionalität minderten.
★★	**schwach** – Die Sicherheitslösung zeigte aufgrund schlechter Bedienbarkeit oder Funktionalität eine mangelhafte oder rudimentäre Leistung in der entsprechenden Kategorie. Einige Produkte mit dieser Bewertung hatten Bugs, die die Produktleistung minderten.
★★★	**durchschnittlich** – Die Sicherheitslösung zeigte eine angemessene Leistung in der entsprechenden Kategorie mit Spielraum nach oben.
★★★★	**gut** – Die Sicherheitslösung zeigte eine gute Leistung in der Kategorie mit nützlichen Features und einer guten Dokumentation.
★★★★★	**außerordentlich gut** – Die Sicherheitslösung zeigte eine hervorragende Leistung in einem Kategoriefeld mit einzigartigen, gut durchdachten oder besonders gut entwickelten Features, die die Benutzerfreundlichkeit und Funktionalität förderten. Außerdem lag eine ausgezeichnete Dokumentation vor.

Vorgehensweise

Passmark Software führte einen Benchmark-Leistungstest und eine subjektive Vergleichsanalyse der Benutzerfreundlichkeit, Schnelligkeit und Effektivität von sieben Business Security-Produkten durch.

Eingesetzte Hardware

Folgende Hardware wurde bei der Vergleichsanalyse und den Leistungstests angewandt und soll eine typische Server- und Businessumgebung repräsentieren.

Server Spezifikationen

Auf dem folgenden Gerät lief ein virtuelles System, auf dem die Serverkomponenten der Sicherheitssoftware installiert wurden:

Betriebssystem:	Windows Server 2003 32-bit
Prozessor:	Intel Xeon CPU @ 3.4 GHz
Motherboard:	Hewlett-Packard 08B4h Festplatte
RAM:	4GB EEC RAM
Festplatte:	Western Digital Raptor 74GB 10,000RPM

Spezifikation der Virtuellen Maschine

Betriebssystem:	Windows Server 2003 32-bit
RAM:	1-2 GB (je nach Produktanforderungen)

Client Spezifikation

Betriebssystem:	Windows 7 Ultimate x64
Prozessor:	Intel Core i7 720 @ 2.67GHz
Grafikkarte:	nVidia GeForce 8800 GT
RAM:	6 GB
Festplatte:	500 GB

Getestete Produkte und Versionen

Produktname	Serverkomponente & Version	Clientkomponente & Version
ESET Smart Security 4 Business Edition	Remote Administrator Console: v4.0.122.0	Smart Security 4 Business Edition: v4.2.40
Kaspersky Business Space Security	Administration Kit: v8.0.2090	Kaspersky Anti-virus 6.0: v6.0.4.1424
McAfee Total Protection for Endpoint	ePolicy Orchestrator: v4.5	McAfee Agent: v4.5.0.1270
Microsoft Forefront Client Security	Forefront Client Security Console: v1.1.1710.90	Forefront Client Security: v1.5.1981.0
Symantec Endpoint Protection	Endpoint Protection Manager: v11.0.600.550	Symantec Endpoint Protection: v11.0.6000.550
Sophos Endpoint Security and Data Protection	Enterprise Console: v4.0.0.2362	Endpoint Security and Control: v9.05
Trend Micro Worry-Free Business Security: Standard Edition	Worry-Free Business Security: v6.0 SP2 build 3025	Client/Server Security Agent: v16.0.3052

Ergebnisse des Benchmark-Leistungstests

Die folgenden Leistungskategorien wurden als praxisnahe Testpunkte ausgewählt, die sich deutlich auf die Systemleistung und Reaktionsgeschwindigkeit von Endpoints auswirken. Diese Eckpunkte erlauben den Vergleich bezüglich des unterschiedlich starken Einwirkens von Business Sicherheitssoftware auf Endpoint-Geräte. Produkte mit guter Performance beeinträchtigen den Arbeitsfluss und die Produktivität nur in geringem Maße.

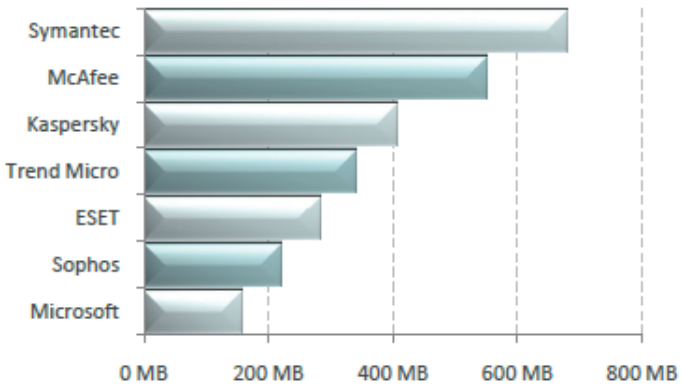
Eine detaillierte Beschreibung der Methodologie finden Sie im Anhang A – Methodologie der Leistungsmessung.

Installationsgröße

Schutz von Endpoints vor übermäßigen Speicherbedarfs

Neuere Versionen von Sicherheitsprodukten zeichnen sich oftmals durch einen gestiegenen Verbrauch an Festplattenspeicher aus, was sich auf viele Endpoint-Geräte problematisch auswirkt. Je umfangreicher eine Installation auf dem Rechner ist, desto mehr Festplattenspeicher wird benötigt – oftmals mehr als notwendig.

Dieser Test misst den gesamten zusätzlichen Festplattenspeicher, der vom Endpoint-Client nach der Installation und einem manuellen Update benötigt wird. Das Endergebnis wird in Megabyte (MB) angegeben.

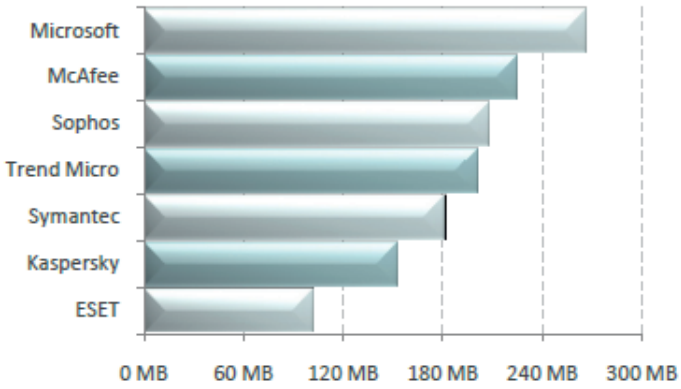


Arbeitsspeicherverbrauch

Wieviele Systemressourcen werden benötigt

Sicherheitsprodukte mit einem enormen Verbrauch an Arbeitsspeicher (bzw. physischem RAM) wirken sich signifikant auf die Leistung von Endpoint-Systemen aus, so dass auf Festplattenlaufwerke mit geringeren Schreib- und Lesegeschwindigkeiten als RAM zurückgegriffen werden muss. Business Sicherheitsprodukte, die viel Arbeitsspeicher verbrauchen, verlangsamen betroffene Endpoints deutlich.

Dieser Test misst den gesamten zusätzlichen Speicherbedarf eines Endpoint-Gerätes im Leerlauf, auf dem ein Endpoint-Sicherheitsprodukt installiert ist. Unser Endergebnis wird in Megabyte (MB) angegeben und bildet den Durchschnitt aus vierzig Messungen.

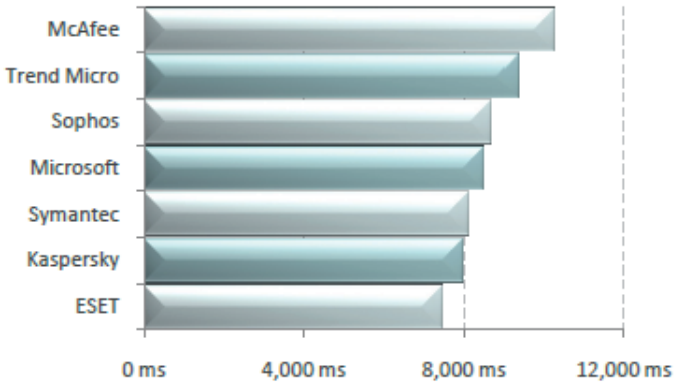


Öffnungsgeschwindigkeit von Word-Dokumenten

Weniger Zeit mit dem Öffnen von Dokumenten verbringen

Sicherheitsprodukte können die Öffnungsgeschwindigkeit von Anwendungen und Dokumenten beeinträchtigen, wenn ihre Anti-Malware-Funktionalitäten, wie Echtzeit-Dateischutz oder Verhaltensanalysen, leistungsarm arbeiten. Langsame Reaktionszeiten von Endpoint-Systemen können so die Produktivität unnötig behindern.

Dieser Test misst die Gesamtzeit, die zum Öffnen eines großen Microsoft Word 2007 Dokuments benötigt wird. Vor dem Öffnen des Programms wurde ein Neustart durchgeführt. Unser Endergebnis wurde in Millisekunden (ms) gemessen und bildet den Durchschnitt aus fünf Messungen.

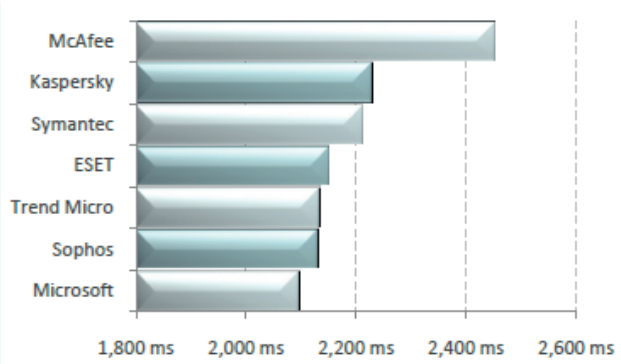


Neustart eines Word-Dokuments

Erneutes Öffnen von Programmen ohne Wartezeit

Das wiederholte Öffnen eines Programms gehört zu den typischen Abläufen von Endpoint-Anwendern, die im Arbeitsalltag häufig zwischen Programmen hin und her wechseln bzw. diese schließen und wieder öffnen. Die Zeit zum erneuten Öffnen einer Anwendung ist ein aussagekräftiger Wert für die Reaktionsgeschwindigkeiten von Endpoint-Systemen.

Dieser Test misst die Gesamtzeit, die zum erneuten Öffnen eines großen Microsoft Word 2007 Dokuments mit unterschiedlichen Medien-Inhalten auf einem Endpoint-System mit installiertem Sicherheitsprodukt benötigt wird. Unser Endergebnis wurde in Sekunden (s) gemessen und bildet den Durchschnitt aus zehn Messungen.

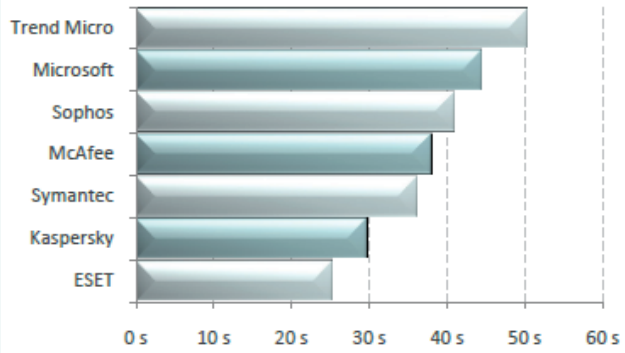


Kopierzeit von kleinen Dateien

Schnelleres Kopieren von Dokumenten

Das Transferieren von Dateien zwischen Geräten und Laufwerken ist eine typische Aktivität von Endpoint-Anwendern. Erweisen sich Funktionen von Business Sicherheitslösungen, wie bspw. Datei-Scan und Heuristik, als leistungsschwach, können sie die Kopierzeit von Dateien negativ beeinflussen.

Dieser Test misst die Gesamtzeit, die benötigt wird, um einen Satz kleiner Dateien von einem Verzeichnis in ein anderes zu kopieren, während ein Endpoint-Sicherheitsprodukt installiert ist. Unser Endergebnis wurde in Sekunden (s) gemessen und bildet den Durchschnitt aus fünf Messungen.

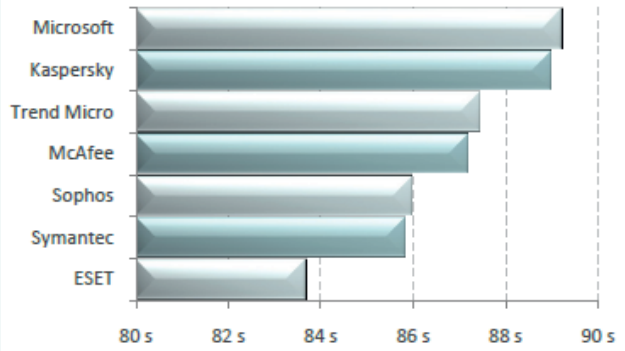


Kopierzeit von großen Dateien

Schnelleres Kopieren von Multimedia-Dateien

Große Dateien zwischen Verzeichnissen hin und her zu kopieren kann ebenfalls von schwachen Anti-Malware-Funktionalitäten installierter Business Sicherheitssoftware behindert werden.

Dieser Test misst die Gesamtzeit, die benötigt wird, um einen Satz großer Dateien von einem Verzeichnis in ein anderes zu kopieren, während ein Endpoint-Sicherheitsprodukt installiert ist. Unser Endergebnis wurde in Sekunden (s) gemessen und bildet den Durchschnitt aus fünf Messungen.

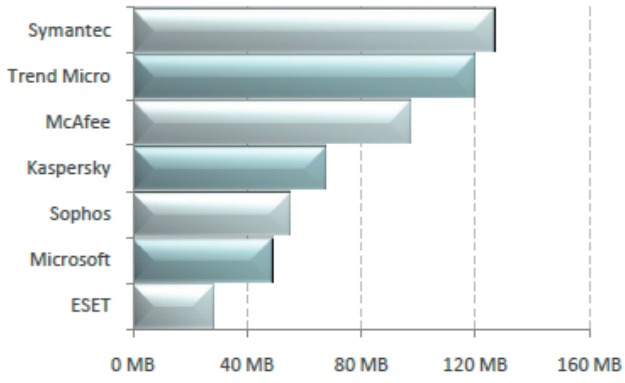


Größe von Client-Signaturdatenbanken

Geringere Belastungen durch Endpoint-Lösungen

Die Datenbankgröße von Anti-Malware-Signaturen auf Endpoint-Geräten ist eine aussagekräftige Variable für die Auslastung der Festplatte durch ein Sicherheitsprodukt.

Diese Test misst die Gesamtgröße von Anti-Malware-Signaturdateien auf einem Endpoint-Gerät nach einem manuellen Update. Unser Endergebnis wurde in Megabyte (MB) gemessen.

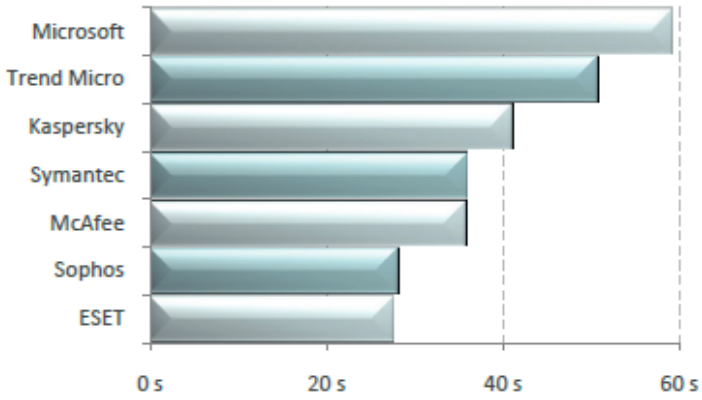


Geschwindigkeit des Systemstarts

Kein langes Warten während des Hochfahrens

Viele Business Software Suites führen während des Systemstarts zahlreiche Aufgaben und Prozesse aus, die die Startzeit erheblich hinauszögern. Der Nutzer kann während dieser Zeit lediglich darauf warten, dass das Gerät irgendwann reagiert. Produkte mit besserer Performance wirken sich dagegen nur geringfügig auf die Geschwindigkeit des Systemstarts aus.

Dieser Test misst die Zeit, die ein Gerät mit installierter Endpoint-Sicherheitslösung zum Systemstart benötigt. Unser Endergebnis wurde in Sekunden (s) gemessen und bildet den Durchschnitt aus fünf Messungen.

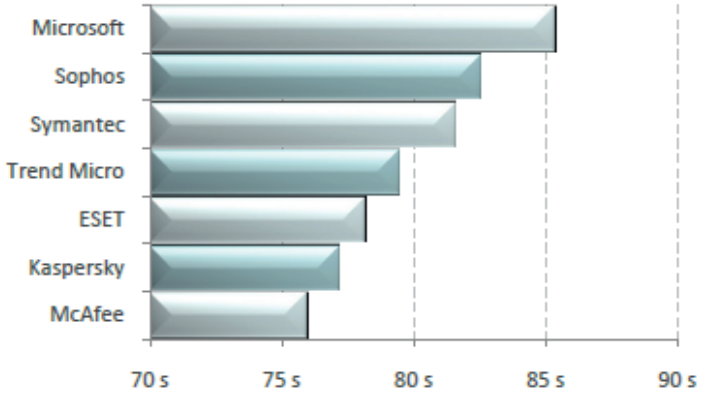


Geschwindigkeit des Neustarts

Weniger Zeit zum Neustart aufwenden

Werden zusätzliche Systemressourcen durch Dienste und Prozesse von Sicherheitsprodukten in Anspruch genommen, verzögert sich das Herunter- und erneute Hochfahren an Endpoint-Geräten.

Dieser Test misst die Zeit, die ein Gerät mit installierter Endpoint-Sicherheitslösung zum Neustart benötigt. Unser Endergebnis wurde in Sekunden (s) gemessen und bildet den Durchschnitt aus fünf Messungen.



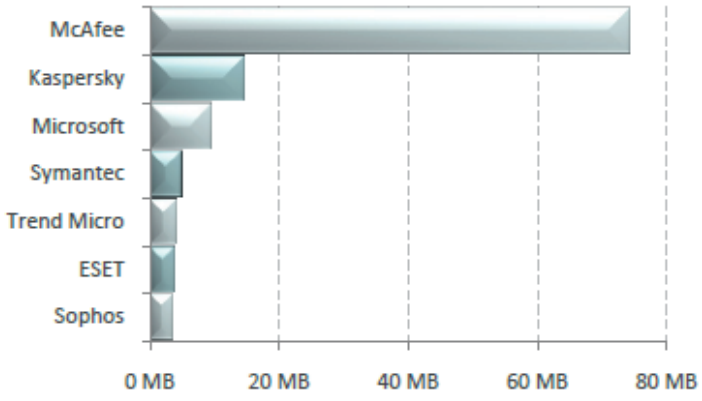
Täglicher Datentransfer

Geringere Belastung des Firmennetzwerks

Alle Sicherheitslösungen benötigen die aktuellsten Signaturen und Aktualisierungen der Scan-Engine, um die verwalteten Netzwerke effektiv gegen Malware zu schützen.

Trotzdem unterscheiden sich Sicherheitsprodukte hinsichtlich der Aktualisierung. Einige Produkte führen inkrementelle Updates durch, während andere wesentlich größere Datenmengen herunterladen.

Dieser Test misst den gesamten, täglich ein- und ausgehenden Verkehr auf dem Server, der durch Engine- und Signaturupdates der Sicherheitssoftware generiert wird. Unser Endergebnis wurde in Megabytes (MB) gemessen und bildet den Durchschnitt aus sechzehn Tagen.



ESET Smart Security Business Edition

Bewertung im Überblick

- Sehr geringe Systembelastung von Endpoint-Geräten. Schnellste und beste Gesamtperformance.
- Geringe Netzwerkauslastung für Updates (durchschnittlich 3-4 MB pro Tag).
- Flexible Verwaltung älterer Versionen und anderer ESET-Produkte für Clients von einer einzelnen, kompatiblen Konsole aus
- Neu zum Netzwerk hinzugefügte Endpoints können automatisch parametrischen Gruppen zugeordnet werden.
- Signaturupdates sind portabel.
- Während einer typischen Installation wird nicht automatisch ein Mirror-Server erstellt.
- Die Benutzeroberfläche der Remote Administrator Konsole ist eher auf Funktionalität als auf Ästhetik ausgerichtet.

Installation und Konfiguration **4/5**

Die Installation der Verwaltungskomponenten von ESET Smart Security 4 Business Edition, nämlich ESET Remote Administrator Server und Konsole, verlief relativ schnell und reibungslos. Nach circa einer Stunde waren Installation und Updates fertig gestellt sowie Grundeinstellungen der Verwaltungskomponenten festgelegt.

Die standardmäßige Installation des Remote Administrators bedurfte kaum Eingriffe seitens des Nutzers, da alle benötigten Komponenten inklusive der eingebetteten Access JET Datenbank nahtlos installiert wurden. Der ESET Remote Administrator Server unterstützt auch andere Datenbanken wie SQL Server, Oracle und MySQL, und kann während der „fortgeschrittenen" Installation die Erstellung einer leeren Datenbank automatisieren. Während der Installation kann der Administrator Passwörter festlegen – dieser Schritt ist jedoch rein optional und Passwörter können auch später eingerichtet werden. Nach der Installation des Remote Administrator Servers dauerte die Installation der Konsole keine zehn Minuten.

Die Kurzanleitung zur Installation und Konfiguration der ESET Smart Security Business Edition war extrem nutzerorientiert. Der „Quickstart Guide" enthielt neben schrittweisen Anleitungen - beginnend mit dem Kauf über das Herunterladen bis zur Einrichtung der Software - auch die geschätzte Dauer eines jeden Steps. Die Anleitung gab auch hilfreiche Tipps für weniger technisch gebildete Nutzer. Zusätzlich bietet ESET ein umfangreiches Handbuch an, das übliche Installationen und erweiterte Produktfunktionalitäten erläutert.

Migration von vorhergehenden Versionen **4.5/5**

Bereits vorhandene Fremdsoftware kann über die Remote Administrator Konsole (mittels Push Installation) entfernt werden, bevor der ESET Client installiert wird. Dazu muss der Administrator zuerst das Removal Tool des Fremdanbieters herunterladen. Zur Vereinfachung bietet ESET dafür eine umfangreiche Linkliste an. Für einige Versionen von ESET Clients führt der Remote Administrator automatisch Upgrades durch. In jedem Fall kann der Remote Administrator alle unterschiedlichen Versionen und Ausführungen von ESET Sicherheitssoftware verwalten. Das Entfernen oder Upgraden installierter ESET Clientsoftware nicht nötig ist.
Das Upgrade auf neuere Versionen des ESET Remote Administrators ist leicht. Administratoren müssen lediglich die neueste Version des Remote Administrators installieren. Die existierende Datenbank sowie alle Einstellungen werden automatisch übernommen. Für Unternehmen mit besonderen Migrations- oder Upgradeansprüchen bietet ESET auch den Komplettaustausch („Rip and Replace" Service) für nordamerikanische Kunden an.

Standard-Policies 4.5/5

Die Grundeinstellungen werden während der Installation des Remote Administrators festgelegt und bilden eine solide Basis für die meisten Verteilungen.

Die Kurzanleitung gibt erste Hilfestellungen für benutzerdefinierte Einstellungen, wie z.B. die Deaktivierung verzichtbarer Meldungen für Endpoint-Geräte.

Installation auf Clients 4/5

Screenshot 1: ESET Smart Security 4 Business Edition (Client)

Die Kurzanleitung liefert eine Checkliste für Punkte, die vor der Installation zu bestätigen sind. Die einzige Einstellung, die in unserem Fall geändert werden musste, war die Deaktivierung des Remote-Registrierungsdienstes auf Endpoint-Geräten.

Nachdem alle Voreinstellungen gesetzt wurden, können Administratoren im Remote Administrationsfenster ein ESET-Installationspaket erstellen. Die Erstellung eines solchen Pakets geht mit fünf Minuten zur Konfiguration auf dem Verwaltungsserver schnell vor sich. Einmal korrekt eingerichtet, kann ein einziges Paket zur Remote Installation auf 32- und 64-Bit Endpoint-Systemen verwendet werden.
Administratoren können den Remote Administrator ebenfalls verwenden, um benutzerdefinierte Installationspakete flexibel durchzuführen. Dies ist auch dann möglich, wenn es sich nicht um ESET-Anwendungen handelt; es muss lediglich eine Installationsdatei im .msi Format vorliegen.

Zielsysteme können mit NetBIOS, IP-Suche oder mit einer vorhandenen Active Directory Struktur identifiziert werden.

Nach dem Start benötigte das Client-Modul etwa zehn Minuten Installations- und Updatezeit auf dem Endpoint-Gerät. Ein Neustart zur Sicherung der Funktionen war nicht nötig.
Größere Verteilungen können mit Hilfe der Windows Gruppenverwaltung durchgeführt werden.
Eine detaillierte Beschreibung befindet sich im Benutzerhandbuch.

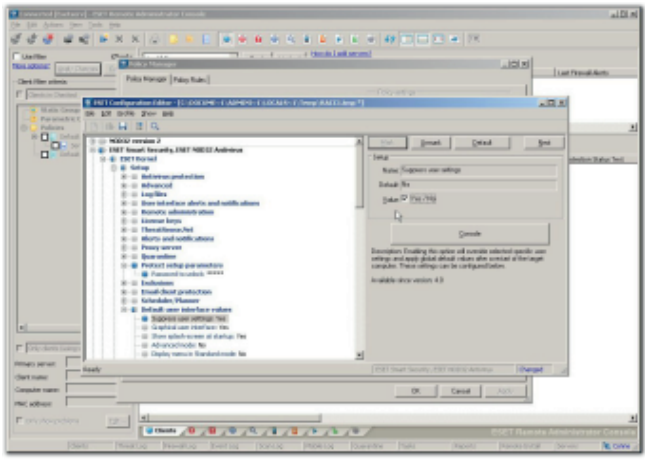
Design der Programmoberfläche 4/5

Die Remote Administrator Konsole erinnert vom Aufbau her an gewohnte Windows Anwendungen. Leider wirkt sie daher etwas farblos und grau, da mehr Wert auf die Funktionalität als auf die Ästhetik gelegt wurde.
Hauptfunktionen sind in Registerkarten angeordnet bzw. über die Menüpunkte auf der Benutzeroberfläche ansteuerbar. Die Navigation ist sehr reaktionsschnell, so dass es Sekunden-Bruchteile dauert, um sich durch Fenster und Menüs zu bewegen.

Die Clientübersicht liefert den Status aller Clients. Übersichtliche Anzeigen geben einen schnellen Überblick über Warnungen, Fehlermeldungen und Alarme für jedes Endpoint-Geräts.

Management von Clients und Policies 5/5

Endpoint-Geräte können manuell in Gruppen eingeordnet werden oder unter bestimmten Voraussetzungen dynamisch zu benutzerdefinierten parametrischen Gruppen hinzugefügt werden. Parametrische Gruppen sind sehr nützlich, denn sie weisen Clients automatisch
Policies für die Verbindung mit dem Server zu oder werden zum Filtern und für das Reporting verwendet.



Screenshot 2: ESET Remote Administrator Console (Server)

Unternehmen mit einer bestehenden Gruppenstruktur, wie z.B. Active Directory, können den Policy Rules Wizard verwenden, um benutzerdefinierte Regeln zu erstellen. Zudem lassen sich Policies existierenden Gruppen und Objekten automatisch zuweisen.
Die Änderung von Policies wird nicht unmittelbar umgesetzt, sondern erst mit der nächsten Verbindung des Clients zum Server. Die Updates der Policies durchgeführt und diese treten dann in Kraft. Möchte der Administrator auf die Standard Policies zurücksetzen, genügt ein einfacher Klick auf „Grundeinstellungen“ im Policy Manager.

Die Remote Administrator Konsole ist voll kompatibel mit den meisten Versionen und auch älteren Ausgaben der ESET-Sicherheitsprodukte. Diese können alle von einer einzelnen Plattform aus verwaltet werden. Die Flexibilität der Remote Administrator Konsole ist besonders für Umfelder geeignet, in denen Client-Upgrades nicht möglich sind. Alle Policies können zur Duplizierung oder für ein Backup als .xml-Datei im- und exportiert werden.

Remote Management 4.5/5

Wenn die Remote Administrator Konsole auf einem Terminal installiert ist, sind alle Funktionalitäten der Remote Verwaltung von Server Modulen möglich. Für den Remote-Zugriff sind keine zusätzlichen Einstellungen des Verwaltungsservers nötig.
Wenn für die Installation des Managementservers die Grundeinstellungen gewählt werden, wird kein Passwort zum Zugriff auf den Server benötigt. ESET empfiehlt jedoch im Handbuch dringend, ein sicheres Passwort anzulegen.

Updates 4/5

Die Grundeinstellungen für Server beinhalten die Einrichtung eines Mirror Servers, von dem Endpoint-Geräte ihre Signaturupdates erhalten. Obwohl der Prozess einfach, gut beschrieben und schnell war, haben andere Produkte die Erstellung eines Updateverzeichnisses während des Installationsvorgangs automatisiert vorgenommen.

Administratoren geben zu Beginn ihren Benutzernamen und das Passwort ein, um auf den ESET Updateserver zugreifen zu können. Diese Informationen werden für spätere Verzeichnisupdates auf dem Managementserver gespeichert.

Alle Signaturdateien, die von ESET Smart Security heruntergeladen werden, können bei Bedarf manuell auf anderen Geräten eingespielt werden. Dies ist vorteilhaft für die Verwaltung von isolierten Netzwerken.

Effektivität 5/5

AV Comparatives verlieh ESET NOD32 Antivirus (v4.0.474.0) im letzten On-Demand Vergleich die Auszeichnung ADVANCED+. Ausschlaggebend war die Gesamterkennungsrate von 97,7% bei nur sehr wenigen Fehlalarmen (“False Positives“). Im Gesamtbericht für 2009 bescheinigte AV Comparatives ESET hohe Erkennungsraten, sehr gute Heuristiken und eine geringe Systembelastung. Aus 16 getesteten Produkten belegte die ESET-Engine den dritten Platz.

Hervorzuheben ist, dass ESET als einziger Anbieter in allen Retrospective/Proactive-Tests von AV Comparatives mit der „ADVANCED+“- Bewertung abschnitt. Seit Beginn der Testreihen von AV Comparatives im Februar 2004 wurden ESET insgesamt 13 ADVANCED+ Bewertungen verliehen. Das entspricht der höchstmöglichen Anzahl von ADVANCED+ Wertungen aus 13 Berichten. Dies macht ESET zum meist ausgezeichneten Anbieter in dieser Kategorie.

Insgesamt schnitten ESET-Produkte seit ihrer Aufnahme in den VB100 (Virus Bulletin) Testreihen 62-mal erfolgreich ab und fielen lediglich dreimal durch.

Das ESET-Vorzeigeprodukt wird seit Mai 1998 getestet und kann die längste Serie von Spitzenbewertungen im VB100-Test mit einer Höchstwertung von 97% vorweisen.

Typische Anwendungsfälle 5/5

Aufgabe	Schwierigkeit	Details
Eine „On-Demand Prüfung“ auf ausgewählten Computern durchführen	einfach	Die On-Demand Prüfung ist eine der zahlreichen voreingestellten Aufgaben in der Remote Administrator Konsole. Sie kann durch Auswahl „Neue Aufgabe“ in der Client Registerkarte durchgeführt werden.
Einen Malware-Bericht „On-Demand“ erstellen und einsehen	einfach	Malware-Berichte findet man in der Registerkarte „Berichte“. Diese können mit Filtern für Ziel-Clients oder bestimmte Bedrohungen angepasst werden. Standardmäßig wird ein HTML-Bericht generiert.
Eine neue Policy erstellen, zuweisen und anwenden	einfach	Der Policy Rules Wizard führt Administratoren durch die Erstellung von Policies. Er wird durch einen Rechtsklick auf Policies aufgerufen.

Kaspersky Business Space Security

Überblick Bewertung

- niedrige Systembelastung auf Endpoint-Geräten, relativ gute Performance
- relativ hoher Traffic durch Verzeichnisupdates
- nutzerorientierte Oberfläche gibt gutes Feedback zum Verlauf und Status von Tasks
- mobile Policies ermöglichen eine flexible Verwaltung je nach Endpoint-Status
- erstes Serververzeichnisupdate verläuft langsam
- Verteilung im Netzwerk dauert relativ lange

Installation und Konfiguration **3.5/5**

Die typischen Vorgänge Installation, Konfiguration und Updates der Management Komponenten von Kaspersky Business Space Security benötigen ungefähr zwei bis drei Stunden. Bereits während der Initialisierung erkannte der Administration Kit Installer, dass Microsoft .NET Framework 2.0 nicht vorhanden war und merkte dieses als Voraussetzung für die Installation an. Die Bestätigung zum Einrichten der fehlenden Komponente startete den .NET Framework Installer und schloss zeitgleich den Kaspersky Administration Kit Assistenten. Nach vollständiger Installation von .NET musste der Kaspersky Administration Kit Installer manuell neu gestartet werden, um den Einrichtungsvorgang fortsetzen zu können.
Dieser wurde nach der kleinen Unterbrechung fortgesetzt. Obwohl nicht im Administration Kit Installer Assistenten integriert, wurde die Installation der SQL Server 2005 Express Edition mit Grundeinstellungen erfolgreich in die Wege geleitet.
Der Quick Start Wizard erschien direkt im Anschluss an die Installation und verlangte nach einen Lizenzkey um die Produkteinrichtung zu ermöglichen. Vor dem Starten des Updateprozesses für den Adminstration Server erstellte der Assistent die Default Tasks und Policies.
Kaspersky stellt für die Installation und die Verwendung der Business Space Security vier technische Dokumentationen zur Verfügung. Diesen Anleitungen fehlt es allerdings stellenweise an Tiefe, einige Inhalte sind doppelt vorhanden. Das durch die Querverweise erzwungene Wechseln zwischen den Dokumentationen machte eine gezielte Informationssuche gelegentlich herausfordernd. Der Quick Start Guide kurz und präzise, in manchen Bereichen wurden Prozesse allerdings allzu sehr vereinfacht.

Migration von vorhergehenden Versionen **4.5/5**

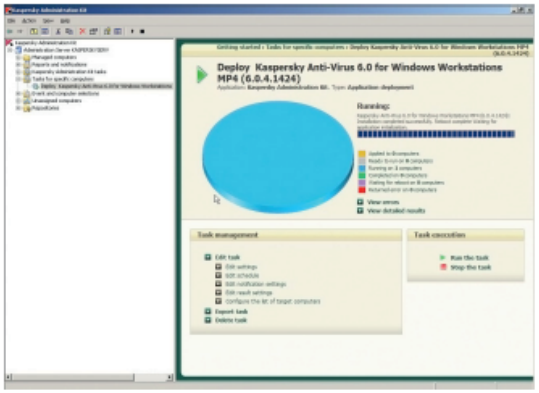
Verglichen mit manch anderen Produkten ist eine Migration des Administration Kit von Version 6 oder höher auf die aktuelle Version recht einfach. Mit einem mitgelieferten Tool müssen Administratoren zuerst ein Backup der vorhandenen Datenbank vornehmen. Alle darin gesicherten Einstellungen und Daten werden dann bei der Installation übernommen. So wird in diesem Fall die Administration Kit Komponente einfach und ohne Deinstallation upgegradet.
Die Client Software Migration ist ebenfalls einfach. Bereits installierte Versionen und Client-Produkte von Kaspersky werden während des Installationsprozesses automatisch deinstalliert.

Mit dem Deployment Wizard können Administratoren vor der Installation von Kaspersky-Lösungen Produkte anderer Anbieter sowie inkompatible Software automatisch entfernen.

Standard-Policies 4/5

Nach der Installation werden vom Quick Start Wizard zwei Policy-Profile angelegt – je eines für Windows Server und Windows Workstations.
Die Default Policies sind gut auf die Rollen der jeweiligen Maschinen abgestimmt.
Die Sicherheitseinstellungen sind ausbalanciert und die Alarmstufen für unterschiedliche Events vordefiniert.

Client Installation 4/5



Screenshot 3: Kaspersky Administration Kit (Server)

Der Deployment Wizard startet nach dem Quick Start Wizard und vereinfacht so den Beginn der Ausrollung selbst für komplett unvorbereitete Personen.

Kaspersky bietet dabei für die Client Installation das beste administrative Feedback aller getesteten Produkte. Mit Kuchendiagramm und Fortschrittsbalken zeigt der Administration Kit den Status der Installationen in „Echtzeit“ an. Nach einigen Minuten erschien es allerdings, als arbeitete diese Statusmeldung nicht immer korrekt.
Der Fortschrittsbalken des Tasks benötigte 25 Minuten, um sich von „Waiting for Application Initialization“ auf „Completed“ zu bewegen – obwohl der Roll Out auf Client-Seite abgeschlossen war und die Lösung scheinbar voll funktionierend zu sein schien. Abgesehen von diesem möglichen Fehler war das Feedback über den Installationsfortschritt eine willkommene Abwechslung.

Der Deployment Wizard bietet auch die Flexibilität, herstellerfremde Applikationen auszurollen und im Hintergrund zu installieren und – bei Bedarf – einen Client neu zu starten.

Die Installation des Kaspersky Clients selbst benötigte rund 15 Minuten und der Zielrechner muss zum Abschluss der Einrichtung neu gestartet werden.

Design der Programmoberfläche 4.5/5

Das Interface des Administration Kits ist verhältnismäßig intuitiv bedienbar. Die Baumstruktur auf der linken Seite ermöglicht den Zugriff auf alle wichtigen Bereiche. Das Anzeigefeld auf der rechten Seite bietet die gewünschten Informationen. Insgesamt ist der Aufbau ähnlich einem Webinterface.
Die Verwaltungsoberfläche wird nach erfolgreichem Einloggen in das Administration Kit angezeigt. Der Zustand des Netzwerkes wird – ähnlich einer Ampel – nach Sicherheitseinstellungen rot, gelb oder grün angezeigt. Detaillierte Informationen über den Status einzelner Clients können als Report erstellt werden. Diese sind flexibel und schnell generierbar und bieten zum besseren Verständnis die Möglichkeit, Diagramme zu integrieren.
Der Fortschritt und Status von verteilten Tasks ist gut ersichtlich und scheint grundsätzlich in Echtzeit upgedatet zu werden. Abgeschlossene Aufgaben werden je nach Ergebnis mit einem Häkchen oder einem Kreuz eindeutig gekennzeichnet.

Management von Clients und Policies 4/5

Das Administration Kit bietet Optionen für ein automatisiertes Policy-Management. Beispielsweise kann eine Policy konfiguriert werden, damit diese im Falle eines Malware-Ausbruchs automatisch aktiviert wird. Leider müssen solche Policies manuell von einem Administrator zurückgesetzt werden, wenn diese spezielle Sicherheitseinstellung nicht mehr benötigt wird.
Für Windows Workstations können Sicherheitsrichtlinien auch als „Mobile Policy“ eingerichtet werden. Diese aktivieren sich automatisch, sobald ein Client vom Netzwerk getrennt wird.
Policies werden grundsätzlich sofort auf Clients verteilt.

Administratoren können Status und Umsetzung einer Richtlinie über die Policy-Einstellungen einsehen. Alle Policies können dupliziert, importiert oder in eine Datei (Format: *.klp) exportiert werden.

Remote Management 4/5

Die Kaspersky Administration Kit Console kann sich remote mit jedem Kaspersky Management Server in einem Netzwerk verbinden. Nach erfolgter Verbindung bietet die Konsole die volle Kontrolle über das Management von Clients und Policies.

Die Konsole selbst scheint eine angepasste Version der Microsoft Management Console zu sein. Sie bietet mit der Option, Management Server zu verbinden oder zu trennen, ein einzigartiges Feature im Testfeld.

Updates 2.5/5

Einrichtung und Durchführung der Updates für den lokalen Updateserver benötigte mehr als zwei Stunden. Glücklicherweise können Administratoren während des Updatevorganges normal weiterarbeiten. Der Aktualisierungs-Prozess selbst läuft im Hintergrund weiter.

Die Kaspersky Client-Lösung benötigte rund 20 Minuten für das Update. Etwas verwirrend war die Tatsache, dass der Client sich für Updates aus dem Internet entschied und nicht auf den aktualisierten lokalen Update Server zugriff.

Eine Untersuchung des Sachverhaltes brachte Licht ins Dunkel – bevor ein Client Updates von einem lokalen Server beziehen kann, muss ein Update Task erstellt und verteilt werden.

Effektivität 4.5/5

Im aktuellsten On-Demand-Vergleichstest von AV Comparatives wurde Kaspersky Anti-Virus (v9.0.0.736) mit „ADVANCED+“ ausgezeichnet und erreichte dabei eine totale Erkennungsrate von 97,1% bei einer geringen Anzahl False Positives.

Der letzte Summary Report (2009) von AV Comparatives bescheinigte Kaspersky eine sehr gute Heuristik, gute Erkennungsraten und umfangreiche Schutz-Mechanismen. Das Produkt erreichte von 16 getesteten Lösungen den zweiten Platz.

Eine weitere“ ADVANCED+“-Auszeichnung erreichte Kaspersky Anti-Virus im Retrospective/ProActive Test vom Juni 2010. Kaspersky hat damit insgesamt sieben „ADVANCED+“-Auszeichnungen erzielt und ist damit unter allen getesteten Anbietern auf Rang zwei in dieser Kategorie.

Kaspersky hat bei den VB100-Tests eine Erfolgsquote von 75% (54 Tests bestanden, 18 Tests nicht bestanden) für alle teilnehmenden Produkte.

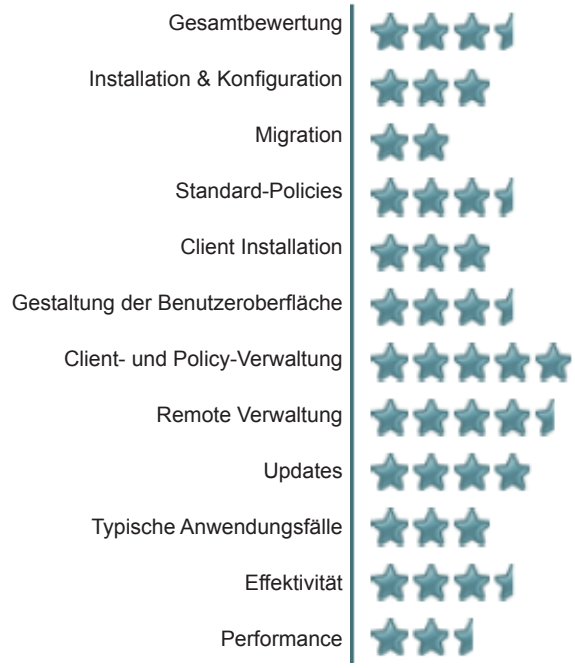
Der aktuellste Misserfolg datiert vom April 2010. Kaspersky Anti-Virus übersah hier einen In-The-Wild-Virus.

Typische Anwendungsfälle 5/5

Aufgabe	Schwierigkeit	Details
Eine „On-Demand Prüfung“ auf ausgewählten Endpoints durchführen	einfach	Für einen On-Demand-Scan wird mit dem Schnellstart-Assistenten automatisch ein Gruppentask erstellt. Dieser Task ist über den Menüpunkt „Managed Computers“ erreichbar.
Einen Malware-Bericht „On-Demand“ erstellen und einsehen	einfach	Malware-Reports sind über den Menüpunkt „Reports and Notifications“ erreichbar. Sie können über das Administration Kit laufend erstellt und eingesehen werden.
Eine neue Policy erstellen, zuweisen und verteilen	einfach	Der „New Policy Wizard“ hilft Administratoren bei der Erstellung neuer Policies. Dieser ist über einen Rechtsklick auf den Menüpunkt „Policies“ erreichbar.

MCAfee Total Protection for Endpoint

Überblick Bewertung



- mäßige Systembelastung auf Endpoint-Geräten mit durchschnittlicher Performance
- höchster getesteter Traffic durch Client Updates
- anfängliche Einrichtung der Tasks und Policies ist kompliziert und erfordert Geduld oder Erfahrung
- eine leistungsstarke Lösung zur Policy-Verwaltung für große Unternehmen und erfahrene Administratoren

Installation und Konfiguration **3.5/5**

McAfee Total Protection und ePolicy Orchestrator benötigten für Installation, Updates und Grundkonfiguration etwa zwei Stunden. Der Installationsprozess verlief zufriedenstellend und ohne großartige Mühen. Ein Großteil der Zeit entfiel auf die Konfiguration von Tasks und Policies für die Verteilung der Clients.

Der ePolicy Orchestrator benötigte praktischerweise keinen Schlüssel für die Installation der Evaluierungsversion. In der Grundeinrichtung wurden automatisch Microsoft SQL 2005 Express, MSXML Parser, Microsoft .NET Framework und MS Visual C++ 2005 mit aufgespielt. Die Komponenten wurden dabei der Reihe nach als Teil des McAfee ePolicy Orchestrators installiert. Dieser Teil der Einrichtung war ein wenig langsam und nach rund 30 Minuten beendet.

Nach Abschluss der Installationsroutine können Administratoren wählen, ob der ePolicy Orchestrator direkt gestartet werden soll. Wir haben dies bestätigt und beim anschließenden Start des ePolicy Orchestrators festgestellt, dass der anschließende Start die Weboberfläche zum Absturz bringt. Das Problem wurde durch manuelles Beenden und Neustarten der Browserinstanz behoben.

Das Benutzerhandbuch bietet detaillierte Schritt-für-Schritt-Anweisungen mit vielen technischen Notizen. Im Gegensatz dazu ist der Quick Overview Guide mehr ein hochentwickeltes Marketing-Instrument als eine nützliche Hilfe für einen schnellen Start.

Migration von vorherigen Versionen **2/5**

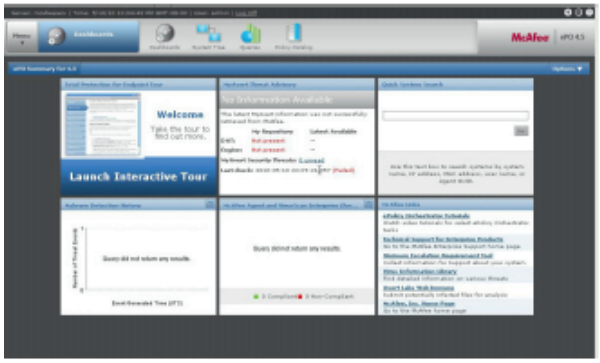
Die Prozedur für ein Upgrade oder eine Migration auf die aktuellste Version des ePolicy Orchestrators ist weder in den Handbüchern noch in der McAfee Corporate Knowledgebase in irgendeiner Art und Weise dokumentiert.

Das Produkthandbuch des ePolicy Orchestrators beinhaltet zwar einige Sätze über Server Tasks mit Bezug auf die Migration früherer Daten (z.B. Host IPS Policy Migration, Event Migration), allerdings finden sich hier keine weiteren Informationen über den Prozess als solchen.

McAfee VirusScan Enterprise prüft Client-seitig nach vorhandener Sicherheitssoftware von Drittherstellern und versucht diese über den Windows-eigenen Uninstaller zu entfernen. McAfee VirusScan ist ebenfalls in der Lage, ältere Versionen von McAfee Client-Lösungen vor der Installation zu entfernen. Diese Vorgehensweise ist im Produkthandbuch gut dokumentiert, allerdings finden sich im ePolicy Orchestrator dazu keinerlei Informationen – auch nicht im Bereich Produktausrollung.

Standard-Policies 3.5/5

Ein paar im Installationsverlauf erstellte Default Policies erscheinen sehr restriktiv. Werden sie nicht geändert, können die restriktiven Regelungen einige Abläufe in einem Netzwerk behindern.
Glücklicherweise bietet das Produkthandbuch entsprechende Empfehlungen, um diese Standard- Policies zu verbessern. So kann zum Beispiel die Default E-Mail-Policy weniger scharf eingestellt werden, indem das Port-Blocking für E-Mail-Server deaktiviert wird.
Einige andere Richtlinien bedürfen für eine ausbalancierte Sicherheit allerdings detaillierter Konfiguration. Ein Beispiel hierfür ist der Passwortschutz für Clients, der nicht autorisierte Änderungen an der Konfiguration unterbindet.



Screenshot 5: McAfee ePolicy Orchestrator (Server)

Installation auf Clients 3/5

Die Verwendung des ePolicy Orchestrators für die Verteilung der McAfee Client-Software innerhalb eines Netzwerkes ist anfänglich kompliziert, speziell für Administratoren, die mit dem Verwaltungsprogramm noch nicht vertraut sind.
Ist die Prozedur allerdings komplett konfiguriert, verläuft die Verteilung des Programmes auf ungeschützten Computer als ein mehr oder weniger automatisierter Prozess.Clients, die noch nicht in die Managementumgebung eingebunden sind, müssen zuerst im Systembaum in Gruppen organisiert werden.
Diese Sortierung kann wahlweise manuell oder auch automatisch anhand von bestimmten Kriterien als Task durchgeführt werden.
Im Anschluss daran muss der Administrator einen benutzerdefinierten Task mit Angabe der auszurollenden Produktversion zur Verteilung der Software erstellen.

Nach Konfiguration und Anwendung wird dieser Task durch den McAfee Agent auf den Clients ausgeführt. Mit Ausnahme von Microsoft Forefront ist dies das einzige Produkt im Testfeld, das die Erstellung zusätzliche Tasks oder Policies voraussetzt, um ein Client Produkt installieren zu können. Die Aufgabe muss anschließend über diese Policies auf ausgewählten Clients oder Gruppen angewendet werden.

Die Aktivierung des McAfee Agents und die folgende Installation der Module benötigten im Anschluss circa 15 Minuten für Installation und Updates.

Design der Programmoberfläche 3.5/5

Alles in allem ist die Benutzeroberfläche des ePolicy Orchestrators überlegt aufgebaut und wirkt aufgeräumt. Auch für den internationalen Einsatz ist das Produkt gut geeignet. So kann der Administrator direkt auf der Login-Seite aus einem von zehn Sprachpaketen wählen.

Ein Download zusätzlicher Komponenten ist dabei nicht erforderlich. Nach erfolgreichem Einloggen erhält der Administrator eine Übersicht über das Netzwerk mit Diagrammen und Quick Links zu allen wichtigen Sicherheitskategorien. Diese Übersicht kann individuell angepasst werden – entweder mit vorgefertigten Layouts oder mit speziell erstellen Datenbankanfragen.
Die Benutzeroberfläche ist relativ ansprechend und stabil für ein Webinterface. Die Navigation bei einem Wechsel zwischen den einzelnen Kategorien ist flott und benötigt nur ein oder zwei Sekunden zur Aktualisierung. Erstaunlich ist der Vergleich mit den Hilfedateien – diese zu Betrachten oder zu Durchsuchen dauert wesentlich länger.

Die wichtigsten Funktionen können über ein Menü am oberen linken Rand erreicht werden. Die einzelnen Menüpunkte sind dabei durch einfach zu erkennende Icons klar und deutlich gekennzeichnet.

Management von Clients und Policies 5/5

Auch wenn die erstmalige Einrichtung von Policies und Tasks für unerfahrene Administratoren möglicherweise abschreckend wirkt, ist McAfee Total Protection for Endpoint nach sorgfältiger Konfiguration in der Lage, viele Prozesse wie die Sortierung von Clients oder die Zuordnung von Policies automatisch vorzunehmen.
Der ePolicy Orchestrator kann gefundene Clients in Gruppen und Untergruppen algorithmisch sortieren. Dieser Algorithmus basiert zum Beispiel auf der IP-Range und speziellen, administrativ festgelegten Tags. Die Policy-Kontrolle ist sehr präzise: Administratoren haben unzählige Möglichkeiten des Fine Tunings für jede einzelne Sicherheitskomponente. Die Tiefe und Fülle an Einstellmöglichkeiten ist – verglichen mit anderen getesteten Produkten – beeindruckend. Für erfahrene Benutzer ist daher die Verwaltung von größeren Umgebungen problemlos möglich.

Ein einzigartiges Feature des ePolicy Orchestrators ist die Möglichkeit, so genannte „Issues“ als Antwort auf verschiedene Events wie Virenbefall oder Monitoring Probleme zu öffnen. Diese Issues sind automatisch an verschiedene Ansprechpartner verteilbar. Sie können dann den Sachverhalten bearbeiten und das entsprechende Ticket erstellen, bearbeiten oder schließen.

Remote Management 4.5/5

Über das Webinterface ist der ePolicy Orchestrator einfach und von jedem Terminal im Netzwerk erreichbar. Auf alle Management-Funktionen kann auf das Webinterface zugegriffen werden. Dafür keine weiteren Konfigurationen am Browser oder Downloads wie ActiveX Controls nötig.

Die Remote-Verbindung zum Management Server ist stabil und geschmeidig. Eine Navigation zwischen Funktionen und dem Erhalten von Daten ist angenehm schnell.

Updates 4/5

Konfiguration und Verwaltung der lokalen Update-Dateien funktioniert einfach über den ePolicy Orchestrator.
Der „Update Master Repository“ Task wird während der Installation des ePolicy Orchestrators erstellt und ermöglicht den täglichen Download neuer Signaturupdates. Der Client Task „Update Client Protection“ wird ebenfalls im Rahmen der Ersteinrichtung erstellt und prüft einmal am Tag, ob neue Downloads zur Verfügung stehen. Diese Prüfung findet zu unterschiedlichen Zeiten statt, um die Netzwerkbelastung minimal zu halten. Die Grundeinstellungen machen für große Umgebungen durchaus Sinn, in kleineren Umgebungen sollten Administratoren die Frequenz der Updates erhöhen. Nur so kann ein umfassender Schutz sichergestellt werden.

Das erste Update der McAfee Client Software vom lokalen Update Server wurde daher manuell angestoßen und benötige rund drei Minuten zur Komplettierung.

Clients, die temporär vom Netzwerk des ePolicy Orchestrator Servers getrennt werden, vollziehen den Update Task ebenfalls. Sie beziehen dabei die Signatur Updates von den McAfee Servern aus dem Internet.

Effektivität 3.5/5

Im aktuellsten On-Demand Vergleichstest von AV Comparatives wurde McAfee AntiVirus (v14.0.306) mit „ADVANCED“ ausgezeichnet. Bei einer totalen Erkennungsrate von 98,9% wurde eine hohe Anzahl an False Positives festgestellt.
Der letzte Summary Report (2009) von AV Comparatives bestätigte diesen Trend, hohe Erkennungsraten mit einer bedauerlicherweise hohen Anzahl False Positives.
Im letzten Retrospective/Proactive Test wurde McAfee Antivirus mit „STANDARD“ ausgezeichnet. Insgesamt hat McAfee Antivirus seit Februar 2004 insgesamt zweimal die Auszeichnung „ADVANCED+“ erhalten.

McAfee hat bei den VB100-Tests eine Erfolgsquote von 70% (48 Tests bestanden, 21 Tests nicht bestanden) für alle teilnehmenden Produkte. In drei dieser Tests wurde McAfee mit zwei Produkten getestet und erreicht damit Rang 6 von sieben in diesem Report getesteten Produkten.

Typische Anwendungsfälle 3/5

Aufgabe	Schwierigkeit	Details
Eine „On-Demand-Prüfung“ auf ausgewählten Computern durchführen	mittel	Administratoren können für diesen Fall den vorkonfigurierten Task für einen On-Demand auf allen oder ausgewählten Clients editieren. Dieser Task muss dabei sofort ausgeführt werden. Leider ist der Status dieses Tasks schlecht einzusehen. Nach Abschluss des Tasks muss dieser wieder auf die Grundeinstellungen zurückgesetzt werden.
Einen Malware-Bericht „On-Demand“ erstellen und einsehen	mittel	Reports werden auf Basis von Abfragen erstellt. Diese liegen dutzendfach vorgefertigt vor und können editiert und ausgeführt werden. Alle Reports werden über den ePolicy Orchestrator generiert und betrachtet.
Eine neue Policy erstellen, zuweisen und anwenden	mittel	Neue Policies können zum Beispiel aus einem Policy Katalog heraus erstellt werden. Die Tiefe der möglichen Einstellungen und Konfigurationen macht allerdings Erstellung, Konfiguration und Zuweisung der neuen Policy ein wenig kompliziert.

Microsoft Forefront Client Security

Überblick Bewertung

- relativ hohe Systembelastung auf Endpoint-Geräten, unterdurchschnittliche Performance
- relativ hoher Traffic durch Serverupdates
- die komplizierte Installation, Konfiguration und Verteilung stellen auch für erfahrene Administratoren eine Herausforderung dar
- die Fehlerbehebung kostet aufgrund der unabhängigen Fehlerprotokollierung jeder Komponente sehr viel Zeit
- beschränkte Möglichkeit On-Demand Tasks vom Verwaltungsserver aus durchzuführen

Installation und Konfiguration **1/5**

Eine typische Installation von Microsoft Forefront Client Security auf einem Server benötigte mehr als einen Tag für die Fertigstellung. Sie erfolgreich abzuschließen war herausfordernd. Ohne ausreichende Erfahrung und großes Wissen über verschiedene Microsoft Server-Komponenten schlägt sie fehl.
Kurz gesagt – Installation und Konfiguration von Microsoft Forefront war die mit Abstand am benutzerunfreundlichste Erfahrung in diesem Testfeld.

Im Gegensatz zum gängigen Prinzip anderer Hersteller, alle benötigten Installer als Pakete anzubieten, geht Microsoft einen kontroversen Weg und bietet diesen in zwei Teile an. Teil eins beinhaltet die grundsätzlichen Installationsmodule und muss zunächst als ISO-Image von der Microsoft Website heruntergeladen und anschließend auf eine CD gebrannt werden. Teil zwei, das Produktupdate für Forefront SP1, wird im Anschluss als separate, ausführbare Datei angeboten.

Das Microsoft Forefront-Setup installiert keine für den Betrieb nötige, voraus zu setzende Komponenten. Diese müssen manuell herausgefunden, heruntergeladen und installiert werden. Die Anzahl der benötigten Bestandteile ist dabei die höchste. Einige Komponenten setzen wiederum andere voraus, die ebenfalls manuell gesucht, heruntergeladen und installiert werden müssen.
Es hat den Anschein als wäre eine Installation von Forefront auch ohne die vorausgesetzten Komponenten möglich (zum Beispiel Windows Software Update Service), allerdings funktioniert in diesem Fall Forefront dann auch nur eingeschränkt.
Das Microsoft TechNet bietet online Dokumentationen für Forefront. Diese sind durchschnittlich aufgebaut, bieten allerdings so gut wie keine Hilfe. Mitunter sind wichtige Schritte für die Installation und Konfiguration einfach nicht vorhanden.

Migration von vorherigen Versionen **1/5**

Für den Migrationsprozess von älteren Forefront-Versionen oder Software von Drittherstellern gibt es im Microsoft TechNet keinerlei Dokumentation. Einige Artikel beschreiben den Prozess zum Entfernen von bestehenden Installationen oder den Migrationsprozess zwischen unterschiedlichen Betriebssystemen bzw. bei Änderungen an der Server-Anordnung.

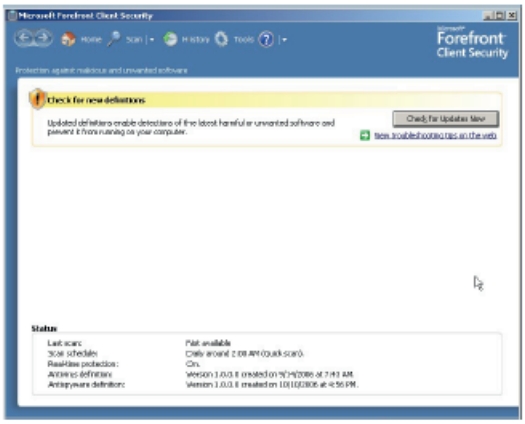
Die wenigen, sich auf Migrationsprozesse beziehenden Dokumentationen erscheinen schwierig und beinhalten – je nach Konfiguration - viele manuell durchzuführende Schritte in einer strikten Reihenfolge. Einige Schritte erfordern unter anderem den Eingriff in die Windows Registry.

Standard-Policies 2/5

Während der Installation der Microsoft Forefront Client Security werden keine Standard-Policies generiert. Eine Gruppenrichtlinie mit Default Settings muss über die Menüpunkte „Policy Management“ und „New“ erstellt werden. Wird diese Richtlinie auf die Clients angewendet, werden Echtzeit-Dateischutz sowie regelmäßige Scans nach Malware und Sicherheitslücken aktiviert.

Client Installation 1/5

Microsoft Forefront Client Security unterstützt eine Verteilung der Client-Software über einige, voneinander unabhängige Windows Komponenten und Dienste. Administratoren müssen eine Default Policy erstellen und verteilen, um die Installation der Client Software zu starten. Einige in diesem Vorgang benötigte Komponenten sind zum Beispiel der Windows Server Update Service (WSUS), der System Management Server (SMS), die Group Policy Management Console (GPMC), die Group Policy Objects (GPO) und der Microsoft Operations Manager (MOM).
Im Rahmen unserer Tests wurden die Nachteile bei der Verteilung über diese Vielzahl von Diensten recht schnell deutlich. Fehlermeldungen verschwinden aus dem Sichtfeld. Jede Komponente verwendete eigene Log-Mechanismen und speichert ihre Logdateien an unterschiedlichen Orten ab. Die Fehlersuche bei einer fehlgeschlagenen Verteilung gleicht somit der Suche nach der Nadel im Heuhaufen. Abhilfe gibt es dafür vereinzelt in verschiedenen Bereichen der Microsoft

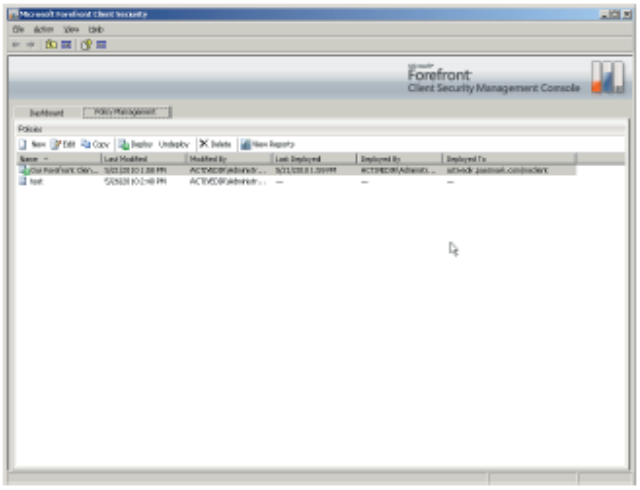


Screenshot 7: Microsoft Forefront Client Security (Client)

TechNet Library.Für Administratoren mit ausgezeichneten Kenntnissen in diversen Windows Modulen ist der Installationsprozess möglicherweise vertrauter. Allerdings benötigen einige dieser „Common Components“ spezielle Einstellungen, die wiederum augenscheinlich den Sinn der Anwendung in Frage zu stellen. So sind beispielsweise Server mit einer existierenden MOM-Infrastruktur nicht in der Lage diese mit Forefront zu nutzen – stattdessen muss eine spezielle Version des MOM für diesen Zweck verwendet werden.

Design der Programmoberfläche 2.5/5

Verglichen mit anderen Produkten im Testfeld fehlen dem Interface der Microsoft Client Security Console viele Funktionen. Die Oberfläche wirkt sehr minimalistisch bestückt. Dies bestätigt sich im Verlauf des Tests: Durch den schlichten Funktionsumfang ist die Console einem Administrator keine Hilfe bei der Verwaltung der zu Grunde liegenden Vielschichtigkeit der Module.
Das Interface verwendet das Microsoft Management Console Framework und bietet mit zwei Reitern Zugriff auf das Policy Management und den Übersichtsbereich. In diesem sind Summary Reports und eine Auflistung von Clients mit Problemen ersichtlich.



Screenshot 8: Microsoft Forefront Security Console (Server)

Management von Clients und Policies 1.5/5

Die meisten Produkte bieten unterschiedliche Möglichkeiten, Gruppen von Clients über deren Sicherheitslösung zu verwalten. Microsoft hingegen vertraut dabei einzig und allein auf die Verwaltungsmöglichkeiten einer bereits bestehenden Windows Server-Infrastruktur. Verwendung finden dabei Group Policy Management (GPM) und das Active Directory.

Die Clients müssen daher in Gruppen oder sogenannten Organizational Units (OU) im Active Directory organisiert sein, bevor eine Policy für Forefront Client Security verteilt und angewendet werden kann.
Das gesamte Policy Management der Forefront Client Security wirkt daher sehr bescheiden. Die einstellbaren Optionen für das Security Management sind limitiert. Das offensichtliche Fehlen detaillierter Einstellmöglichkeiten ist gemessen an der angesprochenen Zielgruppe - Großkunden und Umgebungen mit mehreren Tausend Clients – und der Komplexität des Produktes daher überraschend.
Ferner werden verteilte Policies erst dann angewendet, wenn die Gruppenrichtlinien durch einen Administrator aufgefrischt werden – was allerdings mehrere Stunden dauern kann. Administratoren können ebenfalls mittels Eingabe eines speziellen Befehles ein Update der Forefront Client Security über die Kommandozeile des Computers auslösen. Forefront selbst bietet diese Funktionalität jedoch nicht.

Remote Management 0/5

Microsoft Forefront Client Security unterstützt allem Anschein nach keine zentrale Verwaltung. Ist ein Remote Management möglich, so ist dies in den Dokumentationen der TechNet Library oder in den Hilfedateien nicht erwähnt. Andere Produkte der Forefront Reihe wie der Forefront Threat Management Gateway hingehen unterstützen dem Handbuch nach eine zentrales Management.

Die Autoren der Dokumentationen gehen möglicherweise davon aus, dass Administratoren auf die bereits existierende Remote Desktop Infrastruktur ausweichen und so Fernzugriff auf Produkte mit Forefront Client Security erhalten. Auch wenn moderne Server diverse Remote Desktop Services implementiert haben, sollte diese Möglichkeit der zentralen Verwaltung wenigstens in der Microsoft TechNet Library Erwähnung finden.

Updates 2/5

Um den Management Server der Forefront Client Security als lokalen Update Server verwenden zu können, muss der Windows Server Update Service (WSUS) installiert sein. Da die Aktualisierung der Clients in einem Netzwerk allerdings zeitlich versetzt stattfindet, ist es schwierig vorherzusagen, wann ein ausgewählter Computer seine Programm- und Signaturupdates nun auch wirklich erhält. Daher ist auch die Verteilung von Updates „on-demand“ nur sehr schwierig vom Management Server aus umzusetzen.
Die Client Software der Forefront Client Security enthält einen „Update now“-Knopf, mit dem ein Anwender ein Update anstoßen kann. Leider führte das Drücken des Knopfes zu keinem Ergebnis. Dieses Problem kann umgangen werden, in dem man das erste Update manuell über Microsoft Update herunterlädt.
Da allerdings das erste Update auch Bestandteil der Verteilung ist, fanden wir hier einen weiteren, durch die Vielzahl der bei der Ausrollung verwendeten Komponenten bedingten Stolperstein.

Effektivität 4/5

Im aktuellsten On-Demand-Vergleichstest von AV Comparatives wurde Microsoft Business Essentials (v1.0.1611.0) mit „ADVANCED“ ausgezeichnet und erreichte dabei eine totale Erkennungsrate von 97.1% bei einer sehr geringen Anzahl an False Positives. Der letzte Summary Report (2009) von AV Comparatives bescheinigte Microsoft hohe, proaktive Erkennungsraten und gute Säuberungsqualitäten.

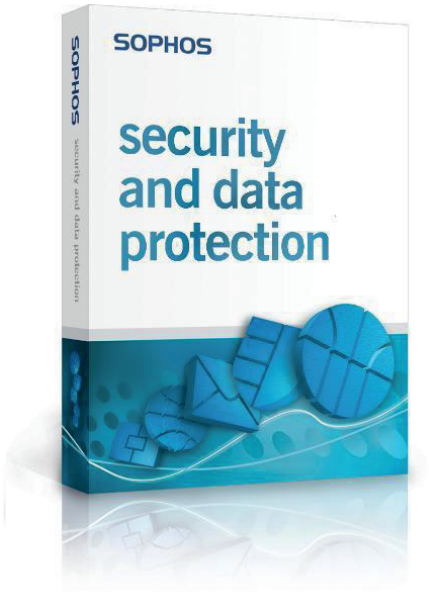
Im letzten Retrospective/Proactive Test wurde Microsoft Business Essentials mit „ADVANCED+“ ausgezeichnet. Insgesamt hat Microsoft seit der ersten Teilnahme drei „ADVANCED+“-Auszeichnungen erhalten und ist damit unter allen getesteten Anbietern auf Rang drei in dieser Kategorie.

Microsoft hat bei den VB100-Tests eine Erfolgsquote von 89% (17 Tests bestanden, 2 Tests nicht bestanden) für alle teilnehmenden Produkte. In einem dieser Tests wurde Microsoft mit zwei Produkten getestet und erreicht damit Rang 2 von 7 in diesem Report getesteten Produkten.

Typische Anwendungsfälle 3/5

Aufgabe	Schwierigkeit	Details
Eine „On-Demand-Prüfung“ auf ausgewählten Computern durchführen	mittel	Ein Administrator kann mit einem Klick auf „Scan now“ einen On-Demand Scan einleiten. Allerdings stehen für die Zielcomputer nur zwei Optionen zur Auswahl – alle Computer oder nur einen einzelnen Computer zu scannen. Dafür kann beim Scan selbst zwischen einem Quick- und einem vollen Scan unterschieden werden.
Einen Malware-Bericht „On-Demand“ erstellen und einsehen	einfach	Reports können von Administratoren direkt auf der Übersichtsseite mit einem Klick auf einen Link erstellt und betrachtet werden. Reports werden standardmäßig im HTML Format erstellt.
Eine neue Policy erstellen, zuweisen und anwenden	kompliziert	Erstellen, zuweisen und verteilen einer neuen Policy ist über den Reiter „Policy Management“ möglich. Ob die neue Richtlinie in einem bestimmten Zeitfenster erfolgreich angewendet wurde oder nicht, ist nur über die Einsicht von verschiedenen Logdateien ersichtlich.

Sophos Endpoint Security and Data Protection



Überblick Bewertung

Gesamtbewertung	★★★
Installation & Konfiguration	★★★½
Migration	★★★★★
Standard-Policies	★★★½
Client Installation	★★★
Gestaltung der Benutzeroberfläche	★½
Client- und Policy-Verwaltung	★★★
Remote Verwaltung	★★★★
Updates	½
Typische Anwendungsfälle	★★★½
Effektivität	★★★½
Performance	★★★

- Moderate Systembelastung auf Endpoint-Geräten. In einigen Bereichen gute Performance, in anderen schlechte Leistung
- der Migrationsprozess von vorherigen Versionen und Fremdsoftware ist gut dokumentiert und unkompliziert
- Updates auf dem Server sind problematisch
- einige Standard-Policies sind zu restriktiv und können wichtige Funktionen stören, wenn sie nicht geändert werden
- die Dokumentation ist auf neun technische Handbücher verteilt

Installation und Konfiguration **3.5/5**

Die vollständige Server-Installation der Management Komponenten von „Sophos Endpoint Security and Data Protection“ benötigte grob zwischen zwei und drei Stunden. Der eigentliche Installationsprozess verlief zügig, das erstmalige Update des lokalen Mirror-Servers hingegen benötigte einen beträchtlichen Teil der Zeit. Der Grund hierfür waren unerklärbare Timeouts beim Aufbau der Verbindung zu den Sophos Update-Servern.

Der Enterprise Console Installer bemerkte nach dem Entpacken der Dateien korrekterweise das Fehlen des Microsoft .NET Framework auf dem Zielsystem und forderte zur Installation der vorausgesetzten Komponente auf. Nach Bestätigung pausierte der Installer der Enterprise Console im Hintergrund und verharrte während der Installation von .NET im Hintergrund. Das gleiche Verhalten beobachteten wir bei der Installation der MS XML- und SQL-Server-Komponenten.
Zum Abschluss der Softwareeinrichtung der Enterprise Console muss sich der aktive Benutzer ab- und wieder anmelden.

Sophos bietet insgesamt neun unterschiedliche Dokumentationen und technische Anleitungen für Installation und Verwendung der Endpoint Security and Data Protection an. Die Advanced Guides sind dabei sehr hilfreich und inhaltsstark. Die Quick Startup Guides sind allerdings durch die sehr knapp gehaltenen Formulierungen eher schwer verständlich und keine große Hilfe.

Migration von vorherigen Versionen **5/5**

Die Migrationsprozesse sind sehr einfach und gut dokumentiert. Sophos bietet für diesen Zweck zwei unterschiedliche Handbücher. Der Quick Upgrade Guide beschreibt den Upgrade-Prozess in Netzwerken mit nur einem Management Server. Der Advanced Guide beinhaltet detaillierte Informationen für komplexere Umgebungen.
Für Standard-Installationen empfiehlt Sophos ein Datenbank-Backup eines unterstützten Produkts, bevor auf eine neuere Version migriert wird. Für andere Komponenten müssen neue Installationspakete heruntergeladen werden. Diese werden im Anschluss ähnlich einer Neuinstallation aktiviert. Alle zuvor vorgenommenen Einstellungen und Policies werden dabei vom Setup-Assistenten entdeckt und unverändert in die neue Version übernommen.

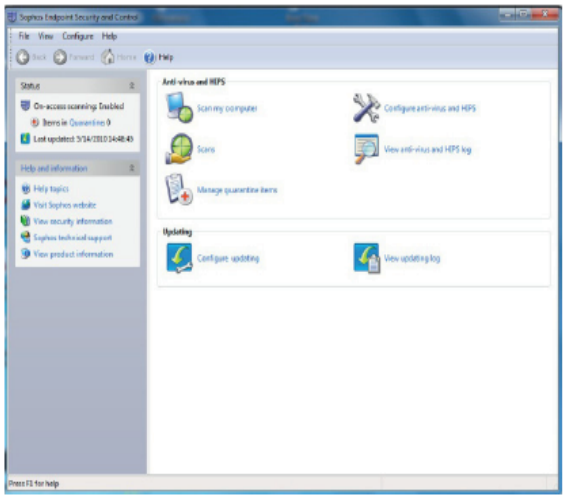
Sophos Endpoint Security kann – wenn dies bei der Verteilung aktiviert wird – auch automatisch Produkte von Drittherstellern erkennen und entfernen. Hier wird ein generelles Removal Tool verwendet. Es existiert allerdings auch ein eigen entwickeltes Programm. Dieses kann weitere Software entfernen, muss allerdings vor der Anwendung konfiguriert werden. Mit dem Third Party Security Software Removal Guide existiert ein Handbuch, das diese Vorgänge dokumentiert.

Standard-Policies 3.5/5

Wird die Firewall-Komponente auf einem Zielcomputer installiert, können die Grundeinstellungen zu starken Einschränkungen in der Konnektivität führen. Die Standard Firewall-Policy ist äußerst restriktiv konfiguriert. Sie blockiert automatisch alle nicht notwendigen und somit einen Großteil der eingehenden und ausgehenden Verbindungen. Sophos weist im Advanced Startup Guide allerdings expliziert auf diese scharfen Einstellungen hin und empfiehlt Administratoren eine Modifikation dieser Richtlinie.
Andererseits sind solch restriktive Richtlinien natürlich sinnvoll. Sie bieten einen guten Schutz für recht viele Netzwerke. Einige spezielle und tiefergreifende Schutzmechanismen wie Data Control, Device Control und Application Control sind standardmäßig deaktiviert.

Client Installation 3/5

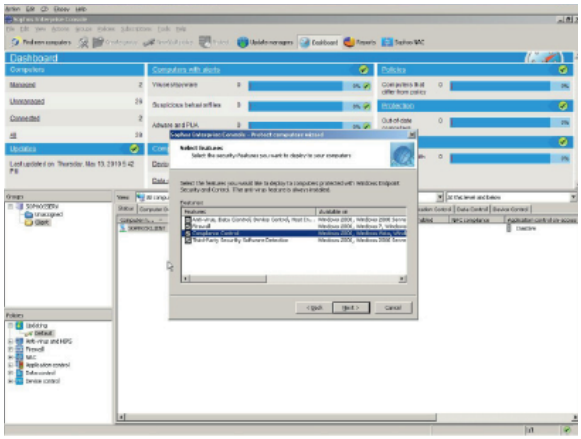
Bezeichnend für die Anzahl der neun unterschiedlichen Handbücher waren auch unsere Erfahrungen mit der Erstinstallation der Clients. Nach Anleitung des Quick Start Guides begannen wir umgehend mit der Verteilung der Software über eine Netzwerkinstallation. Nachdem die Installation auf den Clients zweimal ohne Rückmeldung fehlschlug, zogen wir den Troubleshooting Guide zu Rate – leider ohne Erfolg. Der Advanced Startup Guide offenbarte schließlich die Lösung für dieses Problem.
Für eine erfolgreiche Installation der Software muss der Remote Registry Service auf den Zielcomputern aktiviert



Screenshot 9: Sophos Endpoint Security and Control (Client)

werden. Obwohl der Quick Start Guide normalerweise das erste von Administratoren gelesene Dokument ist, ist diese Voraussetzung dort leider nicht erwähnt.
Der Protect Computer Wizard führt den Administrator durch den Rest der Installation. Nach Auswahl der einzurichtenden Komponenten ist der Prozess recht flott abgeschlossen. Die Silent Installation über das Netzwerk benötigte rund fünf Minuten. Ist das Setup abgeschlossen, wird am Client ein automatisches Update ohne Intervention des Benutzers durchgeführt. Um die Aktualisierung fertig einzuspielen, muss der Client neugestartet werden.

Design der Programmoberfläche 3.5/5



Screenshot 10: Sophos Enterprise Console (Server)

Die Enterprise Console ist praxisnah aufgebaut.
Das Dashboard ist dabei das beständige Element im Interface und ermöglicht Administratoren die Überwachung des Sicherheitsnetzwerkes. Aktive Tasks sind dort ebenfalls aufgelistet. Bei Bedarf kann die Größe des Dashboards geändert werden.
Das Interface-Layout ist gradlinig strukturiert. Bei Bedarf kann sich ein Administrator den Sicherheitsstatus aller Komponenten eines einzelnen Computers anzeigen lassen. Ein Klick auf „Update Manager“ ändert die Übersicht und der Administrator hat Zugriff auf Software Updates, Gruppensortierungen und Policies. Letztere sind dabei auf linksseitig in einer Baumstruktur angeordnet.
Trotz des umfangreich bestückten Dashboards scheint es keinerlei Möglichkeit zu geben, den Status eines On-Demand-Scans zu verfolgen.

Management von Clients und Policies 3/5

Die Verwaltung von Clients und Policies mit Sophos Endpoint Security erweist sich als sehr einfach. Allerdings fehlt es der Lösung letztendlich an der Tiefe und Prozessautomatisierung, wie wir sie bei anderen Lösungen gesehen haben.

Die einzige automatisch durchführbare Funktion der Enterprise Console zur Gruppenverwaltung ist der Download Security Software Wizard. Einmal ausgeführt ist der Wizard in der Lage, eine existierende Domain-Infrastruktur zu importieren und diese im Anschluss zu replizieren. Alle so gefundenen Computer werden dann entsprechend gruppiert. Administratoren haben ansonsten noch die Möglichkeit, neue Computer über Active Directory oder eine Netzwerk- / IP-Range-Suche zu finden.

Ohne Import einer existierenden Active Directory-Umgebung ist aktuell keine andere Option verfügbar, Clients automatisch in Gruppen mit vordefinierten Policies zu sortieren. Nicht zugewiesene Computer müssen dann manuell per Drag & Drop in Gruppen verschoben werden.

Remote Management 4/5

Um den Sophos Server remote verwalten zu können, ist etwas zusätzliche Konfigurationsarbeit über die Enterprise Console des Management Servers nötig. Ein Administrator muss den Remote-Zugriff für ein Konto zuerst über die Zuweisung in die richtige administrative Gruppe freischalten.
Im Anschluss daran muss eine spezielle Installation der Management Console auf dem Terminal durchgeführt werden, von dem aus ein Remote-Zugriff auf den Sophos Server stattfinden soll. Ist das Konto dann mit Zugriffsrechten auf die Datenbank richtig konfiguriert, kann der Client über die Enterprise Console auf alle Management Features remote zugreifen.

Updates 1.5/5

Das erste Update des lokalen Update Servers ist Bestandteil der Grundinstallation und verursachte hier die ersten Probleme.
Nach dem Start der Enterprise Console öffnete der Download Security Software Wizard eine Popup-Fenster, in dem der Administrator die von Sophos gelieferten Zugangsdaten für die Download Server eingeben muss. Der Wizard war anschließend nicht in der Lage, eine Verbindung zu den Sophos Update Servern herzustellen. Auch nach mehrmaligen Versuchen kam es immer wieder zu Server Timeout Fehlermeldungen. Basierend auf Informationen aus dem Sophos-Forum versuchten wir eine Reparaturinstallation der Update Manager Komponente.
Diese brauchte augenscheinlich den gewünschten Erfolg und wir benötigten für das erste Update Zeit und Bandbreite. Der Vorgang benötigte mehr als 30 Minuten und zum Abschluss wurden insgesamt rund 200 MB Updates übertragen. An einigen Stellen erhielten wir eine nicht eindeutige Fehlermeldung. Die Download Security Software Komponente meldete, sie wäre nicht in der Lage, das Update herunterzuladen. Es wurde empfohlen, den nächsten automatischen Downloadzeitpunkt abzuwarten, um den Download fertigzustellen. Nachdem die Fehlermeldung geschlossen wurde, verschwand der Punkt „Run the Download Security Software Wizard“ aus den Aktionsleisten und es gab offensichtlich keinen Weg, den Updateprozess manuell noch einmal zu starten. Alle Clients hingegen konnten direkt nach der Installation ohne Probleme ihre Updates beziehen.

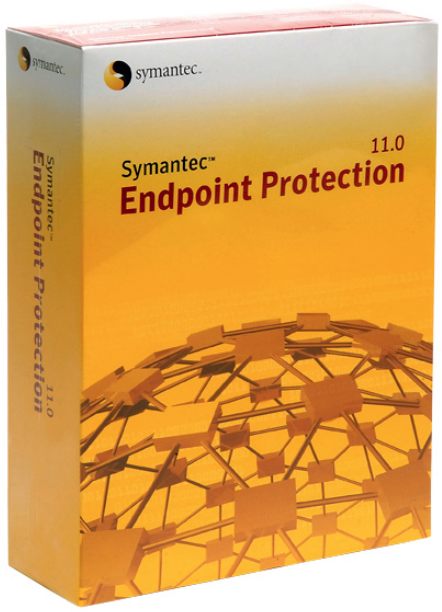
Effektivität 3.5/5

Im aktuellsten On-Demand Vergleichstest von AV Comparatives wurde Sophos Antivirus (v9.03) mit „ADVANCED“ ausgezeichnet. Bei einer totalen Erkennungsrate von 93,7% wurde eine sehr geringe Anzahl an False Positives festgestellt.
Der letzte Summary Report (2009) von AV Comparatives bescheinigt Sophos relativ gute Erkennungsraten. Verglichen mit anderen Produkten in unserem Report sind wir allerdings der Meinung, dass eine Erkennungsrate von 93,7% vergleichsweise gering ist – jeder 20. Virus könnte nicht erkannt werden.
Im letzten Retrospective/Proactive Test im Juni 2010 wurde Sophos Anti-Virus mit „ADVANCED“ ausgezeichnet. Sophos hat bis jetzt in dieser Kategorie noch keine „ADVANCED+“-Auszeichnung erhalten. Sophos hat bei den VB100-Tests eine Erfolgsquote von 77% (52 Tests bestanden, 16 Tests nicht
bestanden). Seit der ersten Teilnahme im Januar 1998 ist Sophos mit nur einem Produkt getestet worden.

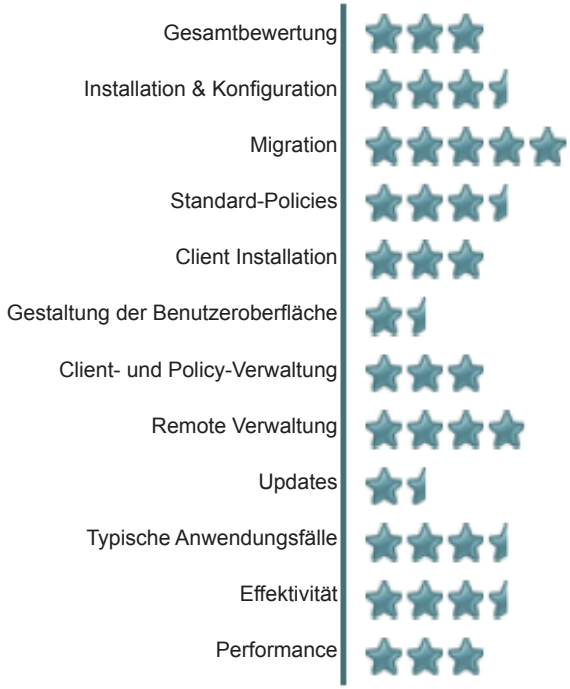
Typische Anwendungsfälle 3.5/5

Aufgabe	Schwierigkeit	Details
Eine „On-Demand-Prüfung“ auf ausgewählten Computern durchführen	mittel	Ein Administrator kann mit einem Rechtsklick auf einen Zielcomputer aus der Enterprise Console heraus einen vollen System Scan starten. Die Console gibt allerdings kein unmittelbares Feedback über das Ergebnis dieser Aktion. Eine Auswahl der Scanparameter ist nicht möglich.
Einen Malware-Bericht „On-Demand“ erstellen und einsehen	einfach	Ein Klick auf die Leiste „Reports“ öffnet den Report Manager. Um einen Report on-demand zu erstellen, muss ein Anwender ein Template auswählen und anschließend den Reporting Prozess starten.
Eine neue Policy erstellen, zuweisen und anwenden	einfach	Mit einem Rechts-Klick auf die Kategorie „Security“ und den Menüpunkt „Neu“ wird eine neue Policy erstellt. Ein Doppelklick auf die neu erstellte Richtlinie öffnet den Policy Wizard und erlaubt detaillierte Änderungen.

Symantec Endpoint Protection



Überblick Bewertung



- Unterdurchschnittliche Systembelastung von Endpoint-Geräten
- Moderate Netzwerkauslastung durch Mirror- Updates
- Malware Erkennungsrate wurde von unabhängigen Testfirmen als sehr hoch eingestuft
- Flexibles Policy Management und Verteilung von Endpoint Clients und Speicherplätze
- Das Abrufen und Weiterverteilen von Signaturupdates an Endpoint-Geräte ist leicht einzurichten
- Die Manager Konsolenoberfläche ist ein wenig schwerfällig
- Der Wechsel von Produkten anderer Hersteller wird nicht unterstützt

Installation und Konfiguration **3.5/5**

Die Installation und Konfiguration der Verwaltungskomponenten von Symantec Endpoint Protection dauerte von Anfang bis Ende ungefähr zwei Stunden. Der Symantec Endpoint Installationsassistent benötigt auf dem Server einen aktivierten IIS World Wide Wide Web Publishing Dienst (WS3SVC). Dieser wird als Server Role vom Windows Server Management hinzugefügt.

Wir haben dann den Endpoint Protection Installationsassistenten manuell neu gestartet, woraufhin er uns problemlos durch den restlichen Prozess führte. Symantec Endpoint Protection verlangte nicht einmal einen Registrierungscode, um die Installation abzuschließen. Nach der Beendigung richtete der Konfigurationsassistent des Management Servers eine eingebettete Datenbank mittels integriertem Installer ein.

Nach der Grundinstallation haben die Administratoren die Möglichkeit, Migrations- und Verteilungsassistenten auszuführen oder direkt weiter zur Managementkonsole zu gehen.

Insgesamt waren die Handbücher für den Installationsprozess gut geschrieben, boten genaue schrittweise Anleitungen. Diese berücksichtigten die Benutzeroptionen in allen Phasen der Installation und enthielten Empfehlungen für typische Ersteinrichtungen.

Migration von vorherigen Versionen **3.5/5**

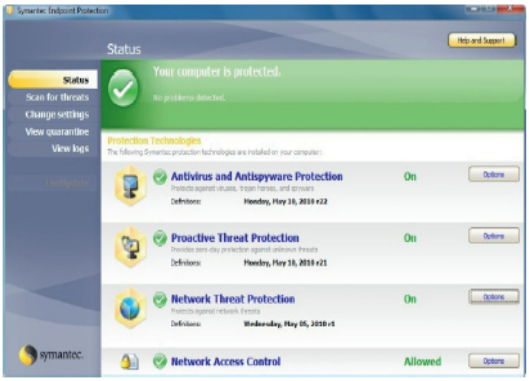
Die Migration anderer Versionen oder Varianten von Symantec Produkten wird angemessen unterstützt. Manches davon ist auf der Symantec Support Webseite sehr gut durch FAQs und Online-Präsentationen dokumentiert. Die Webseite bietet Administratoren einen schnellen Zugang zu Informationen über Migrationspfade der Produkte, „Vorher-Nachher“-Snaphots der Server-Hierarchie, Aufgaben vor und nach der Migration und über die Preisgestaltung.
Eine kurze Anleitung zum Migrationsprozess findet sich im Installationshandbuch. Bei kompatiblen Varianten älterer Symantec Server-Software erkennt die Installation vorhandene Einstellungen und exportiert diese in die neue Produktversion. Es ist nicht nötig, bestehende Serverkomponenten zu löschen. Sobald das Server-Upgrade vorgenommen wurde, führt der Server mittels der AutoUpgrade-Funktion eine automatische Aktualisierung der Endpoint-Geräte durch.
Unternehmen, die eine ältere Version von Symantec Antivirus nutzen, können bestehende Gruppen und Policies mittels des Migrations - und Verteilungsassistenten übernehmen.
Leider sind weder Material noch Support für das Upgrade von Drittprodukten erhältlich.

Standard-Policies 3.5/5

Die meisten Sicherheitseinstellungen werden durch Standard-Policies definiert. Der voreingestellte Schutz von Endpoints ist ausgewogen. Er soll für den Nutzer „unauffällig“ sein: Zum Beispiel werden in Quarantäne gesetzte Dateien auf Client-Geräten repariert und wiederhergestellt.
Firewall Voreinstellungen sind nicht offensichtlich restriktiv, so dass Endpoint-Anwender normalen Zugang zum Internet und zu internen Netzwerken haben. Die einzigen Bereiche, in denen Policies nicht während der Installation erstellt werden, sind die Gerätesteuerung und Ausnahmefälle.
Administratoren können aus drei präfigurierten Einstellungsprofilen für den Antiviren- und Antispyware Schutz auswählen: ausgewogener Schutz, Hochleistungsschutz oder Hochsicherheitsschutz. Als Standard-Einstellung ist der ausgewogene Schutz aktiviert.
Wenn neue Einstellungen an Endpoint-Geräten vorgenommen werden sollen, muss der Administrator auf den nächsten Aktualisierungskreislauf warten, der die neuen Policies an die Endpoints verteilt. Wir haben festgestellt, dass die Einstellung „automatisch aktualisieren“ in der Verwaltungskonsole auf „nie“ gesetzt ist. Wenn der Administrator diese Voreinstellung nicht ändert, werden neue Policies weder heruntergeladen noch ausgeführt.

Installation auf Clients 3/5

Der Migrations- und Verteilungs- Wizard ist in der Lage, ein Installationspaket zu erstellen. Dies kann im gesamten Netzwerk angewendet werden und lässt dem Administrator die Wahl zwischen „unbeaufsichtigter“ oder Hintergrundinstallation.



Screenshot 11: Symantec Endpoint Protection (Client)

Die für diese beiden Optionen verwendeten Bezeichnungen können verwirrend sein. Wenn eine „unbeaufsichtigte“ Installation ausgewählt wird, ist das Client Software-Installationsprogramm auf dem Endpoint Gerät sichtbar. Es zeigt den Verlauf der Installation an, bevor es den Endpoint-Nutzer auffordert, das Gerät neu zu starten. Umgekehrt findet eine stille Installation im Hintergrund statt, ohne dass eine Aufforderung zum Neustart erscheint oder eine Interaktion des Anwenders erforderlich wäre. Es dauert weniger als drei Minuten, das Installationspaket zu erstellen. Danach erkennt der Push Deployment Wizard nicht verwaltete Endpoints mittels NetBIOS und bestehende Gruppenstrukturen, wie etwa Active Directory, IP-Adresse oder Host-Name. Diese Geräte können auch über die Management-Konsole über die IP-Adresse oder den Host-Name gefunden werden.
Die Verteilung verlief nicht stabil, da die remote Verteilungsanwendung (ClientRemote.exe) zusammenbrach, ohne dem Administrator ein Feedback über das Troubleshoot-Log zu geben. Dieses Problem wurde durch einen Neustart des Management-Servers gelöst.
Einmal verteilt, benötigte das Client Paket etwa vier Minuten und einen Neustart des Gerätes, um die Installation zu beenden.

Design der Programmoberfläche 3.5/5

Die Symantec Endpoint Protection-Konsole verliert durch ihre Schwerfälligkeit und die lange Reaktionszeit. Generell ist sie über die Benutzeroberfläche langsam zu steuern und benötigt einige Sekunden, um Daten abzurufen oder zwischen Kategorien und Anwendungen zu wechseln. Das erste Laden einer Kategorie dauert am längsten, während sich bei den folgenden Zugriffen die Reaktionszeit verbessert. Die geringe Geschwindigkeit der Management-Konsole führen wir darauf zurück, dass sie sich zwar als Windows-Applikation ausgibt, aber langsamer Web-Technologien bedient.
Die Kategorien der Registerkarten sind kurz und bündig gehalten. Die Überschriften von Tasks sind entweder beschrieben oder Aufgaben-basiert. Dies ermöglicht eine relativ intuitive Ausführung der üblichen administrativen Aufgaben. Auf der Home-Registerkarte befindet sich ein zusammenfassendes Dashboard. Der Administrator kann auch auf der Monitore-Registerkarte nach spezifischen Einträgen und Tortendiagrammen suchen.
Als eher unbedeutender Punkt wäre anzuführen, dass der Task-Wizard - obwohl er nützlich bei der Migration, bei der Client-Verteilung und bei Backups ist - nicht direkt von der Management-Konsole aus zugänglich ist.

Management von Clients und Policies 4/5

Die Management-Konsole bietet relativ detaillierte Policy-Verwaltungsoptionen für Endpoint-Geräte und -Orte. Gemeinsame Policies sind Standard und können für jede Gruppe oder jeden Standort angewendet werden. Im umgekehrten Fall sind individuelle Policies spezialisierter und lassen sich nur für eine Gruppe anwenden, wenn sie sich an einer spezifischen Stelle befindet.Gruppen können aus bestehenden organisatorischen Strukturen importiert werden, wie etwa LDAP oder einem Active Directory Server. Andernfalls müssen Gruppen manuell vor der Client-Installation dem Client-Baumdiagramm hinzugefügt werden. Die Symantec Endpoint Verwaltungskonsole erlaubt dem Administrator flexible Wechsel zwischen Push- und Pull-Modi für die Policy-Verteilung. Für verschiedene Orte können unterschiedliche Modi eingestellt werden. Diese Eigenschaft ist praktisch, da sie es dem Administrator ermöglicht, die Verteilung von Policies an die gegebenen Netzwerkbedingungen und der Größe der Verteilung anzupassen.

Remote Management 4.5/5

Auf den Management-Server kann remotemäßig mit dem Symantec Protection Manager Webzugang zugegriffen werden. Dazu sind lediglich der korrekte Benutzername und das Passwort erforderlich.
Es sind keine zusätzlichen Anpassungen der Benutzerkonten oder von Browserkomponenten notwendig. Die Web Acces Remote-Konsole ist voll funktionsfähig und gleicht der Management-Konsole auf dem Management-Server. Diese arbeitet auch hier beim Navigieren zwischen Kategorien und Rubriken etwas langsam.

Updates 5/5

Das Herunterladen und Verteilen von Updates an Clients ist mühelos und verlangt sehr wenig Konfiguration.

Der Management-Server wird während der Installation als zentrale Datenbank eingerichtet, von der die Clients Updates automatisch abrufen. Meistens sind die Voreinstellungen bereits optimal und erfordern keine weiteren Konfigurationen vom Administrator. Für größere Verteilungen können Administratoren andere Server als Plattform für Gruppenupdates festlegen. Diese agieren dann als Verteiler, indem sie Updates vom Verwaltungsserver abrufen und an Knotenpunkte verteilen.

Verglichen mit anderen Lösungen ließ sich das Update der Symantec Client-Lösung vom Management-Server aus schnell durchführen.

Effektivität 5/5

Der aktuellste On-Demand-Vergleichstest von AV Comparatives verlieh Norton Antivirus (v17.5.0.127), aufgrund weniger False Positives und einer Gesamterkennungsrate von 98.6 % die „ADVANCED+“-Auszeichnung.

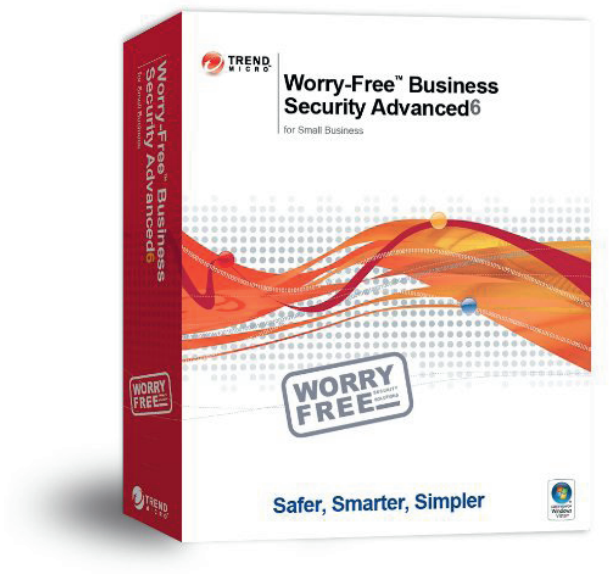
Der letzte Summary Report (2009) von AV Comparatives stellte fest, dass Symantec sehr hohe Erkennungsraten erzielte, eine geringe Systembeeinträchtigung ausübte und über eine hohe Benutzerfreundlichkeit verfügte. In diesem Bericht belegte Symantec den ersten Platz von sechzehn getesteten Produkten.

Der Retrospective/Proactive Test vom Juni 2010 beurteilte Norton Anti-Virus mit “ADVANCED”. Bislang hat Symantec nie eine „ADVANCED+“-Klassifizierung in dieser Kategorie erhalten.
Insgesamt hat Symantec den VB100-Test 54-mal bestanden und ist 7-mal durchgefallen. Mit einer Erfolgsquote von 88% erreichte Symantec die drittbeste Gesamtbewertung im VB100-Test.

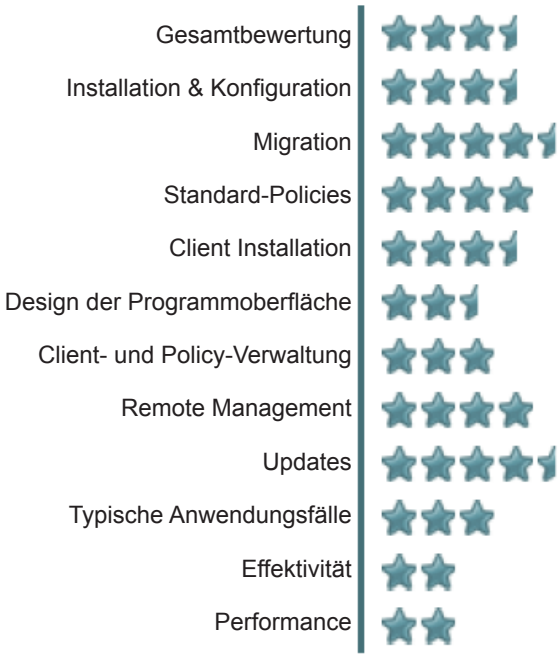
Typische Anwendungsfälle 4/5

Aufgabe	Schwierigkeit	Details
Eine „On-Demand Prüfung“ auf ausgewählten Endpoints durchführen	leicht	In der Client-Registerkarte mit einem Rechtsklick auf die Gruppe oder den Zielcomputer „Befehl auf Gruppe anwenden >Scan“ aktivieren. Die Management-Konsole bietet drei Scanoptionen an: Aktiv, komplett oder benutzerdefiniert. Die Ausführung kann unter „Befehlsstatus“ überprüft werden.
Einen Malware-Bericht „On-Demand“ erstellen und einsehen	mittel	In der Registerkarte „Berichte“ können Administratoren den Berichtstyp und den Berichtszeitraum auswählen. Berichte werden per Voreinstellung im HTML-Format erstellt und nehmen einige Zeit in Anspruch, wenn man sie on-demand generiert.
Eine neue Policy erstellen, zuweisen und anwenden	leicht	In der Registerkarte „Policies“ wählen Sie die relevante Sicherheitskategorie und klicken rechts auf „hinzufügen“ einer neuen Policy. Die neue Policy kann einer Gruppe oder einem Ort zugewiesen werden.

Trend Micro Worry Free Business Security



Überblick Bewertung



- Relative hohe Systembeeinträchtigung auf Endpoint Geräten, unterdurchschnittliche Performance.
- Relativ geringe Netzwerkauslastung durch Server updates Migration von Vorgängerproduktenwird gut unterstützt
- Zu schlichte Client- und Policy-Verwaltung, die für kleinere Unternehmen besser geeignet wäre
- „Outbreak Defense“ handhabt einen potentiellen Virenausbruch im Netzwerk ohne Eingriff des Nutzers
- Störungen der Grafik verschlechtern den guten Eindruck der Benutzeroberfläche

Installation und Konfiguration **3.5/5**

Eine normale Installation der Management-Komponenten von Trend Micro Worry-Free Business Security („Evaluations-Version“) benötigte etwa zwei Stunden.

Während die Installation ohne Probleme voranschritt, verlangte der Installationsassistent nur ein moderates Eingreifen seitens des Benutzers. Diese wenigen Fälle hätte man entweder aus dem Installationsprozess herausnehmen können oder in die Konfigurationsphase verschieben können.
Beispielsweise wird vom Anwender verlangt, vor dem Aufspielen der Software einen Pre-Scan durchzuführen. Gleichzeitig soll er aber auch Angaben zu seinem Unternehmen geben.

Ein oder zwei Installationsscreens mangelte es an Detailgenauigkeit. Zum Beispiel verlangte die Eingabeaufforderung „Komponenten auswählen“ eine Benutzeraktivität, erklärte aber die Funktionen dieser Komponenten nicht.

Der Worry-Free Business Security Installer installierte automatisch das .NET Framework und den Apache Web Server als integrierte Bestandteile der Hauptinstallation. Die Testversion von Worry-Free verlangte keinen Lizenzschlüssel, um mit der Installation fortzufahren.

Trend Micro bietet keine Kurzanleitung an. Das Installationshandbuch verfügt über alle benötigten Informationen, inklusive einer schrittweisen Anleitung für alle Installationsarten.

Migration **4.5/5**

Der Migrationsprozess wird von Trend Micro Worry Free Business Security angemessen unterstützt.

Lediglich einige ältere Versionen von Trend Micro Business Security-Produkten werden beim Upgrade auf Worry-Free Business Security unterstützt. Bei unterstützten Produktvarianten ist das Upgrade ähnlich leicht durchzuführen wie eine Standardinstallation. Auch die Identifizierung des Security-Servers gelingt einfach.

Auf Client-Seite wird die Migration der meisten Varianten von Trend Micro-Produkten sowie Software von Fremdanbietern unterstützt. Wird eine Trend Micro-Lösung vom Client Deployment erkannt, wird ein Endpoint-Upgrade durchgeführt. Bereits vorhandene Antivirensoftware anderer Hersteller wird vor der Installation des Trend Micro-Clients entfernt.

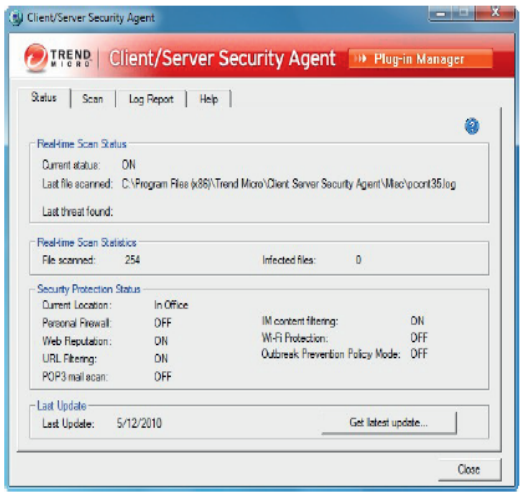
Standard-Policies 4/5

Worry-Free Business Security ist mit Voreinstellungen ausgestattet, die auf die Standardnutzung abgestimmt sind. Abhängig davon, ob eine klassische Installation ausgewählt oder ein Upgrade durchgeführt wurde, können die Voreinstellungen leicht variieren.

Die standardmäßigen Policy-Optionen für Sicherheitskomponenten sind abhängig von der Funktion oder vom Standort einer Gruppe. So könnte beispielsweise bei Desktop-Gruppen das Behaviour Monitoring aktiviert sein, während es bei Server-Gruppen deaktiviert ist. Die Firewall und die POP3-Prüfung sind jeweils per Voreinstellung deaktiviert. Bei Aktivierung besitzt die Firewall Standardeinstellungen für typische Anwendungsszenarien von Endanwendern, wie z.B. dem Webzugang.

Installation auf Clients 3.5/5

Die Verteilung des Client/Server-„Security Agents“ im Netzwerk war relativ einfach. Jedoch war dieser Prozess in der Anleitung nicht vollständig dokumentiert, so dass die Problemlösung erschwert wurde. Das Administrator-Handbuch erwähnt die Notwendigkeit, zunächst den Remote Registry Service auf Windows Vista Clients zu aktivieren. Wir haben jedoch festgestellt, dass dies auch auf Geräte mit Windows 7 zutrifft.



Screenshot 13: Trend Micro Client/Server Security Agent (Client)

Endpoint-Geräte können mit NetBIOS, Active Directory oder per Namenssuche gefunden werden.

Unsere Verteilung im Netzwerk war in weniger als fünf Minuten abgeschlossen. Worry-Free Business Security bietet eine Anzahl verschiedener Methoden der Client-Verteilung, so dass sie flexibel an die Bedürfnisse eines Unternehmens angepasst werden kann. Automatisierte Verteilungsmethoden beinhalten die Agent-Installation für ungeschützte Computer, die sich auf der Domain mit einem Login Script von Worry-Free Business Security anmelden. Andere Methoden erfordern die Mithilfe der Endanwender. Zum Beispiel werden sie aufgefordert, das Agent-Paket von der internen Worry-Free Business Security Seite, die beim Setup angelegt wurde, oder über einen E-Mail Link herunterzuladen und zu installieren.

Design der Programmoberfläche 2.5/5

Als Web-Oberfläche kommt die Trend Micro Worry-Free Business Security Konsole schnörkellos daher. Unglücklicherweise stellten wir bei manchen Elementen der Konsole Störungen der Grafik fest, die die ansonsten reibungslose und reaktionsschnelle Handhabung beeinträchtigen. Dieser Makel wurde besonders deutlich, als wir versuchten, Sicherheitseinstellungen zu konfigurieren. Nachdem wir einige Elemente angeklickt hatten, war die Oberfläche mit defekten Registerkarten und ausgeklappten Grafiken übersät.

Ein weiterer Nachteil der Worry-Free Business Security Web-Oberfläche war der notwendige Download der ActiveX-Komponente „AtxEnc“, bevor auf die Konsole zugegriffen werden konnte. Darauf wird in der Dokumentation von Trend Micro jedoch nicht explizit hingewiesen. Es wird lediglich erwähnt, dass die Web-Konsole ActiveX als Internet-Technologie verwendet.
Die Management-Funktionen mit aufklappbaren Kategorien sind über die Toolbar im oberen Bereich des Programmfensters intuitiv zugänglich. Die Statusübersicht wird beim Anmelden als Hauptfenster geöffnet und zeigt den Netzwerkstatus der Geräte und den Bedrohungsstatus an. Diese Informationen werden nicht in Echtzeit dargestellt. Administratoren können das Dashboard manuell aktualisieren, wann immer sie Informationen abrufen wollen.

Management von Clients und Policies 3.5/5

Worry-Free Business Security verfügt über eine angemessene Anzahl von Sicherheitseinstellungen. Jedoch verliert sie Punkte durch ausschließlich gruppenspezifische Policies. Außerdem ist es nicht möglich, bestehende Infrastrukturen zu importieren und Endpoints automatisch in Gruppen einteilen zu lassen.
Trotzdem kann Worry-Free Business Security ein einzigartiges Feature zur Client-Vewaltung vorweisen. „Outbreak Defense“ reagiert automatisch auf weltweite Virenausbrüche, die von Trend Micro festgestellt werden. Wann immer ein Ausbruch auftritt, nimmt Trend Micro eine Präventivmessung vor, um das Netzwerk vor einer Infektion durch die spezifische Malware zu schützen. Vorbeugende Maßnahmen zur Erhöhung der Sicherheitsstufe beinhalten das Sperren von gemeinsam genutzten Dateien, Schreibschutz für bestimmte Ordner, das Blocken von Ports und eingeschränkten Zugriff auf Endpoint-Clients.
Für jede Sicherheitskomponente von Worry-Free Business Security gibt es eine große Anzahl von Einstellungsoptionen. Auch die Policies sind flexibel einstellbar. Korrekt konfiguriert können verschiedenen Modulen „Out of Office“-Policies zugewiesen werden, wenn beispielsweise Endpoints vom Server getrennt werden.

Remote Management 3,5/5

Der Remote-Zugriff auf den Worry-Free Business Security Server ist einfach. Über die Web-Oberfläche kann auf den Management-Server zugegriffen werden, ohne dass weitere Konfigurationen vorgenommen werden müssen. Insgesamt können alle Arbeiten zufriedenstellend erledigt werden. Alle Funktionen sind zugänglich und der Anwender kann relativ schnell zwischen den Kategorien und Funktionen wechseln.

Wie bereits erwähnt, ist die zusätzliche Installation eines ActiveX-Add-ons erforderlich, um den Zugriff auf die Web-Konsole zu ermöglichen. Dies sollte im Handbuch präziser dargestellt werden. Bei keiner anderen Sicherheitslösung im Test war eine zusätzliche Browser-Installation nötig.

Updates 4.5/5

Die Aktualisierung von Worry-Free Business Security ist einfach. Bei der Installation der Management-Software wird der Server so konfiguriert, dass er stündlich nach Updates auf dem Trend Micro Active Update Server sucht, diese herunterlädt und so als zentrale Speicherstelle für Updates von Endpoints fungiert.

Das erste Client-Update nach der Installation ist ebenso einfach. Standardmäßig führt der Client/Server-Agent vor der ersten Inbetriebnahme automatisch Updates der Virendefinitionen durch. Dies sichert den Client von Anfang an.

Die Worry-Free Business Security-Konsole ermöglicht es Administratoren außerdem, Clients auf das neueste Update zu synchronisieren oder ein Rollback durchzuführen.

Effektivität 2/5

Die aktuellste On-Demand Vergleichstest von AV Comparatives verlieh Trend Miro Antivirus (v17.50.1366.0) den „TESTED“-Rang, da eine große Anzahl an Fehlalarmen auftraten und eine Gesamterkennungsrate von 90.7 % ermittelt wurden.
Diese Erkennungsrate war die niedrigste verglichen mit allen anderen getesteten Anbietern und Produkten.

Im aktuellen Summary Report (2009) von AV Comparatives sind keine Testergebnisse für Trend Micro-Produkte zu finden.

Der Retrospective/Proavtive-Test vom Juni 2010 bewertete Trend Micro mit „STANDARD“. Seit der Einführung dieses Tests im Februar 2004 hat Trend Micro noch keine „ADVANCED+“-Klassifizierung in dieser Kategorie erreicht.

Trend Micro hat den VB100-Test 16-mal bestanden und ist 11-mal durchgefallen. Somit erzielte es eine Gesamterfolgsrate von 59 %. Trend Micro hat die letzten drei Tests seit April 2008 nicht bestanden und zog die Produkte von der Teilnahme am VB100-Test zurück.

Typische Anwendungsfälle 3/5

Aufgabe	Schwierigkeit	Details
Eine „On-Demand Prüfung“ auf ausgewählten Endpoints durchführen	leicht	On-Demand Scans können durch Klicken auf die Scan -Kategorie und Auswahl des manuellen Scans ausgeführt werden. Administratoren können lediglich Computergruppen für den Scan auswählen. Es können viele Scanoptionen und –Arten festgelegt werden.
Einen Malware-Bericht „On-Demand“ erstellen und einsehen	mittel	Ein einmaliger Bericht kann vom Menüpunkt „Berichte“ aus erstellt werden. Leider können Berichte nur im PDF Format erstellt werden.
Eine neue Policy erstellen, zuweisen und verteilen	mittel	Eine bestehende Policy für eine Gruppe zu bearbeiten, gestaltet sich wesentlich einfacher, als eine neue Policy zu erstellen, zuzuweisen und zu verteilen.

Haftungsausschluss und Bekanntmachung

Dieser Bericht behandelt ausgewählte Produkte für Unternehmenssicherheit, die im Testzeitraum erhältlich waren. Die Versionsnummern der in diesem Dokument untersuchten Software können im Abschnitt „Getestete Produkte und Versionen“ eingesehen werden. Mit Ausnahme der Ergebnisse des Performance-Tests und der Produkteffektivität, die mit quantitativen Messungen erhoben wurden, spiegeln die aufgeführten Produktbewertungen die subjektive Sicht von PassMark Software bezüglich der Erfahrungen beim
Installieren, Konfigurieren und Anwenden jedes Produktes wider.

Haftungsausschluss

Obwohl jede Anstrengung unternommen wurde, um sicherzustellen, dass die in diesem Bericht aufgeführten Informationen zutreffend sind, übernimmt PassMark Software Pty Ltd keine Verantwortung für Fehler, Auslassungen oder veraltete Informationen und haftet nicht für direkte, indirekte, zufällige und folgende Schäden oder Bußzahlungen, die aus der Verfügbarkeit, der Nutzung, dem Zugriff auf oder dem mangelnden Zugriff auf diese Informationen resultieren.

Bekanntmachung

Die Anfertigung dieses Berichts wurde von ESET LLC gefördert.

Schutzmarken

Alle Schutzmarken sind Eigentum ihrer jeweiligen Inhaber.

Kontaktdaten

PassMark Software Pty Ltd
Suite 202, Level 2
35 Buckingham St.
Surry Hills
Sydney, Australia

Fon: +61 (2) 96900444
Fax: 61 (2) 96900445

Web: www.passmark.com

Anhang A –Performance Methodologie der Leistungsmessung

Erstellung des Client-Images

Nach der Installation des Client-Images wurden die nachfolgenden Windows-Dienste/Features deaktiviert, um die Auswirkungen durch die Hintergrundaktivitäten von Windows zu minimieren und die Validität der Testergebnisse sicher zu stellen:

- Windows SuperFetch - deaktiviert für alle Tests. Wieder eingeschaltet, um eine Optimierung der Bootzeit zu ermöglichen.
- Microsoft Search Indexer - deaktiviert für alle Tests
- Windows Sidebar - deaktiviert für alle Tests
- Windows Defender - deaktiviert für alle Tests
- Windows Updates – Zunächst werden Windows Updates installiert. Vor den Baseline-Tests wurden die Windows Updates deaktiviert und blieben während der gesamten Testdauer ausgeschaltet.

Nach der Installation jedes Sicherheitsprodukts auf dem Endpoint-Gerät wurden Schwankungen der Client-Aktivität begrenzt, indem Produktupdates und automatische oder geplante Prüfungen deaktiviert wurden.
Vor dem Versuch wurde außerdem Microsoft Word auf den Endpoint-Geräten installiert, um den Test zur Öffnungsgeschwindigkeit von Dokumenten durchführen zu können.

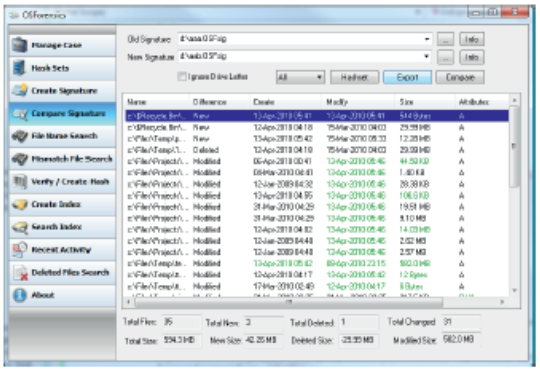
Installationsgröße (Endpoint)

Beschreibung

Dieser Test misst den gesamten zusätzlichen Festplattenspeicher, den die Endpoint Client-Komponente nach der Installation benötigte.

Test Tool(s)

OSForensics (ehemals OSCheck) von: PassMark Software
Neue Version einer Software, die kürzlich von PassMark Software entwickelt wurde. Derzeit öffentlich erhältlich als OSCheck auf der PassMark Website: http://www.passmark.com/products/oscheck.htm OSCheck wird verwendet, um Signaturen von Laufwerken, Ordnern und Dateien zu erfassen und zu vergleichen. So können Vergleiche von Dateien anhand zweier Signaturen gezogen werden, um neu erstellte, bearbeitete oder gelöschte Ordner zu identifizieren.



Screenshot 15: PassMark OSForensics

Methodik

- OSForensics wurde zur Erstellung einer Laufwerks-Signatur verwendet, um einen Basiswert zu erhalten.
- Die Client Komponente des Security Produkts wurde auf dem Endpoint Gerät installiert.
- Wo es möglich war, wurde das Paket über das Netzwerk installiert, das heißt von der Server Komponente über das Netzwerk an die Client-Geräte verteilt. Die Verteilung über das Netzwerk spiegelt die normale Nutzung im realen Umfeld wider.
- Wo es möglich war, hat PassMark während des Installationsprozesses voreingestellte Standard-Optionen gewählt.
- Nach der Installation führte PassMark ein manuelles Update der Client Software durch und startete das Endpoint-Gerät neu, um temporäre Dateien zu löschen.
- Nach dem manuellen Update und dem Neustart wurde eine zweite Disk-Signatur erstellt.
- Die Laufwerks-Signaturen wurden mit Hilfe von OSForensics verglichen,um die Größe der hinzugefügten oder bearbeiteten Dateien und Ordner zu ermitteln.

Ergebnis

Das Endergebnis ergab sich aus der ermittelten Gesamtmenge zusätzlicher und veränderter Dateien (größere Dateien) nach der Client Installation, dem manuellen Update und dem Neustart des Gerätes.

Arbeitsspeicherverbrauch (Endpoint)

Beschreibung In diesem Test wurde der gesamte zusätzliche Speicherbedarf gemessen, den ein Endpoint-Gerät mit installierter Sicherheitssoftware während eines Systemleerlaufs verbrauchte.

Test Tool(s) SysinfoAvg von: PassMark Software
Ein von PassMark Software entwickeltes Dienstprogramm mit Kommandozeilen, das den Arbeitsspeicherbedarf von Windows ermittelt und protokolliert
(z.B. Gesamtverbrauch, Verbrauchsspitzen, etc.)

Methodik
- Vor dem Test wurde das Endpoint-Gerät für fünf Minuten im Leerlauf belassen, um die Beeinträchtigung durch Systemstart und Hintergrundprozessen zu verringern.
- SysinfoAvg wurde konfiguriert, den Arbeitsspeicherbedarf 5 Minuten lang im 15-Sekunden-Takt zu ermitteln und zu protokollieren. So wurden 20 Proben pro Testdurchgang genommen.
- Der Test wurde beim ersten und fünften Durchgang durchgeführt, so dass sich zwei Durchgänge und insgesamt 40 Proben ergaben.

Ergebnis Das Endergebnis wurde in Megabytes (MB) gemessen und als Mittelwert aus 40 Stichproben errechnet. Dieser Durchschnitt wurde vom Basiswert subtrahiert, um den gesamten zusätzlichen Speicherbedarf zu ermitteln.

Öffnen und Neustart eines Word-Dokuments (Endpoint)

Beschreibung Dieser Test misst die Gesamtzeit, die zum erneuten Öffnen eines großen Microsoft Word 2007 Dokuments mit unterschiedlichen Medien-Inhalten auf einem Endpoint-System mit installiertem Sicherheitsprodukt benötigt wird.

Test Tool(s) AppTimer von: PassMark Software
Ein Testwerkzeug, das von PassMark entwickelt wurde und die Öffnungsgeschwindigkeit einer Windowsanwendung misst und protokolliert. Der AppTimer kann hier heruntergeladen werden: http://www.passmark.com/products/apptimer.htm

Methodik
- Der AppTimer wurde zum Öffnen eines großen Dokuments konfiguriert.
- Wir haben „groß“ definiert als ein Word-Dokument mit Medienmix und einer Größe von 980KB.
- Das Dokument lag im .docx Format vor und wurde in Microsoft Word 2007 (v1.2.0.4518.1014) geöffnet.
- Zu Beginn jedes Durchgangs wurde das Gerät für fünf Minuten im Leerlauf belassen, um eine Beeinträchtigung durch den Systemstart oder Hintergrundprozesse zu vermeiden.
- Nach fünf Minuten wurde mit dem AppTimer das Dokument insgesamt dreimal geöffnet und geschlossen.
- Der Test bestand aus fünf Durchgängen, wobei nach jedem Durchgang ein Systemstart durchgeführt wurde. So soll die Beeinflussung durch möglicherweise noch im Cache vorhandene Windows-Anwendungen minimiert werden.
  Insgesamt ergaben sich 15 Testergebnisse.
- Aus 15 Ergebnissen:
  - repräsentierten 5 Ergebnisse die Öffnungsdauer nach einem Systemstart. Diese Ergebnisse fielen langsamer aus, da Windows das Dokument noch nicht im Cache hatte. Von den 15 Ergebnissen sind dies das die 1., 4., 7., 10. und 13.
  - repräsentierten 10 Ergebnisse die Öffnungsdauer ohne Systemstart. Von den 15 Ergebnissen sind dies das 2., 3., 5., 6., 8., 9., 11., 12., 14. und 15.

Testdatei(en) Ein 980 KB großes Microsoft Office Word Dokument im DOCX Format.

Ergebnis Unsere Endergebnisse wurden in Millisekunden (ms) gemessen und sind der Durchschnitt aus zehn Proben. Der Test ergab zwei unterschiedliche Messgrößen:
- Öffnungsgeschwindigkeit eins Word-Dokuments: Das Endergebnis war der Durchschnitt aus fünf Messungen (von 15), genauer die 1., 4., 7., 10. und 13.
- Neustartgeschwindigkeit eines Word-Dokuments: Das Endergebnis war der Durchschnitt aus 10 Messungen (von 15), genauer die 2., 3., 5., 6., 8., 9., 11., 12., 14. und 15.

Kopierzeit für kleine Dateien (Endpoint)

Beschreibung	Dieser Test misst die Gesamtzeit, die benötigt wird, um einen Satz kleiner Dateien von einem Verzeichnis in ein anderes zu kopieren, während ein Endpoint-Sicherheitsprodukt installiert ist.
Test Tool(s)	CommandTimer von: PassMark Software Eine von PassMark Software entwickelte Kommandozeilen-Anwendung, die die Geschwindigkeit einer Aufgabe bei Eingabeaufforderung misst und protokolliert.
Methodik	- Zu Beginn jedes Durchgangs wurde das Gerät für fünf Minuten im Leerlauf belassen, um eine Beeinträchtigung durch den Systemstart oder Hintergrundprozesse zu vermeiden - Der CommandTimer misst die Zeit, die zum Kopieren einer kleinen Anzahl größerer Dateien in ein anderes Verzeichnis auf einem lokalen Laufwerk gebraucht wurde. Dazu wurde der Befehl xcopy verwendet. - Der Test bestand aus fünf Durchgängen mit einem Neustart nach jedem Durchgang
Testdatei(en)	Ein Satz von 821 Dateien, insgesamt circa 659 MB groß. Dieser Satz soll eine große Menge von kleinen Dateien repräsentieren, die auf einem durchschnittlichen PC zu finden ist. Er enthielt verschiedene Dateiformate, wie Windows Systemdateien (DLL, EXE, CPL, UCE, etc.), Bilddateien (GIF, JPG, PNG),Filmdateien (AVI, WM, RM), Musikdateien (MP3), Office-Dokumente (PPT, PPTX, DOCX, DOC, XLS) und PDFs
Ergebnis	Unser Endergebnis wurde in Sekunden (s) gemessen und bildet den Durchschnitt aus fünf Proben.

Kopierzeit für große Dateien (Endpoint)

Beschreibung	Dieser Test misst die Gesamtzeit, die benötigt wird, um einen Satz großer Dateien von einem Verzeichnis in ein anderes zu kopieren, während ein Endpoint-Sicherheitsprodukt installiert ist.
Test Tool(s)	CommandTimer von: PassMark Software Eine von PassMark Software entwickelte Kommandozeilen-Anwendung, die die Geschwindigkeit einer Aufgabe bei Eingabeaufforderung misst und protokolliert.
Methodik	- Zu Beginn jedes Durchgangs wurde das Gerät für fünf Minuten im Leerlauf belassen, um eine Beeinträchtigung durch den Systemstart oder Hintergrundprozesse zu vermeiden - Der CommandTimer misst die Zeit, die zum Kopieren einer kleinen Anzahl größerer Dateien in ein anderes Verzeichnis auf einem lokalen Laufwerk gebraucht wurde. Dazu wurde der Befehl xcopy verwendet - Der Test bestand aus 5 Durchgängen mit einem Neustart nach jedem Durchgang
Testdatei(en)	Ein Satz von 11 Dateien, insgesamt circa 2,5 GB groß. Dieser Satz soll eine Menge von Dateien repräsentieren, die auf einem durchschnittlichen PC zu finden ist. Er enthielt verschiedene Dateiformate, wie Dateidaten (DAT), große Bilddateien (BMP, JPG), Dokumentdateien (PDF, TXT), große Archivdateien (ZIP) und ausführbare Dateien (EXE).
Ergebnis	Unser Endergebnis wurde in Sekunden (s) gemessen und bildet den Durchschnitt aus fünf Proben.

Geschwindigkeit des Systemstarts (Endpoint)

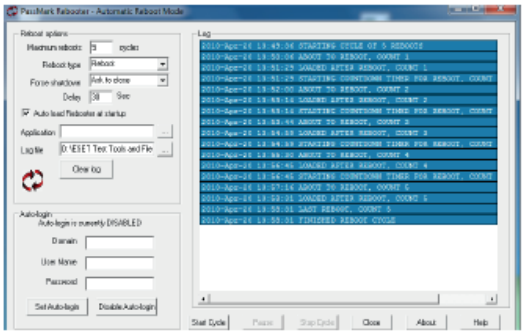
Beschreibung	Diese Metrik misst die Zeit, die ein Gerät mit installierter Endpoint-Sicherheitslösung zum Systemstart benötigt.
Test Tool(s)	Xbootmgr und xperf von: Microsoft Diese Tools sind im Windows Performance Toolkit Version 4.6 enthalten (Bestandteil von Microsoft Windows 7 SDK, erhältlich auf der Microsoft Webseite). Xbootmgr wurde genutzt, um den Bootprozess optimieren und die Zeit zum Hochfahren zu messen. Xperf wurde benutzt, um die Daten von xbootmgr zu analysieren.

Methodik

- Netzwerkverbindungen wurden getrennt, um Störungen zu vermeiden
- Der Windows-Dienst SuperFetch wurde vor dem Test aktiviert, um sicherzustellen, dass die Optimierung des Systemstarts fehlerfrei läuft. Während des Tests wurde der Dienst wieder abgestellt, um die Hintergrundaktivität zu minimieren
- Xbootmgr wurde vor dem Test benutzt, um eine Optimierung des Systemstarts mit dem Befehl „xbootmgr.exe-trace boot-prepSystem“ durchzuführen. Die Optimierung gewährleistet zuverlässige Ergebnisse.
- Nach der Optimierung wurde ein Benchmark-Test mit dem Befehl „xbootmgr.exe-trace boot – numruns 5“ durchgeführt
- Der xbootmgr Befehl startet das System fünf Mal in Folge und zeichnet die Boot-Spuren auf
- Mit xperf wurden diese Spuren analysiert ein Boot-Wert wurde ermittelt. Dieser Wert steht für die Zeit, die zum vollständigen Systemstart benötigt wird.

Ergebnis

Unser Endergebnis wurde in Sekunden(s) gemessen und bildet den Durchschnitt aus fünf (5) Proben.



Screenshot 16: PassMark Rebooter

Geschwindigkeit des Neustarts (Client)

Beschreibung

Diese Metrik misst die Zeit, die ein Gerät mit installierter Endpoint-Sicherheitslösung zum Neustart benötigt. Wir haben die Zeit gemessen, die vom Befehl „Neustart“ bis zur vollständigen Nutzbarkeit vergeht.

Test Tool(s)

Rebooter von: PassMark Software
Ein Werkzeug, das von PassMark entwickelt wurde, um die Zeit zu messen, die für einen kompletten Neustartprozess benötigt wird. Der Rebooter kann von unserer Webseite heruntergeladen werden:
http://passmark.com/products/rebooter.htm

Methodik

- Netzwerkverbindungen wurden getrennt, um Störungen zu vermeiden
- Vor dem Versuch wurden Bootzeit-Tests durchgeführt. Vor diesen wurde zur Optimierung xbootmgr.exe angewandt. SuperFetch wurde ebenfalls aktiviert, um den fehlerfreien Ablauf der Optimierung zu gewährleisten
- Mit dem Rebooter wurde das Gerät neu gestartet und die Zeit dafür gemessen
- Das Gerät wurde fünf Mal neu gestartet, so dass sich fünf Testergebnisse ergaben

Ergebnis

Unser Endergebnis wurde in Sekunden (s) gemessen und bildet den Durchschnitt aus fünf (5) Proben.